

Komunikace mezi doménami s různou bezpečnostní klasifikací



HP ProtectTools a HP SecureSolutions

Bezpečnostní seminář Multi-Level security

Marta Vohnoutová

Listopad 2013

Problém přístupu k doménám s různou bezpečnostní klasifikací

Problém chytré horákyne

Protichůdné požadavky:

•Aplikační

- Umožnit přenos dat mezi systémy
- Komunikovat

•Bezpečnostní

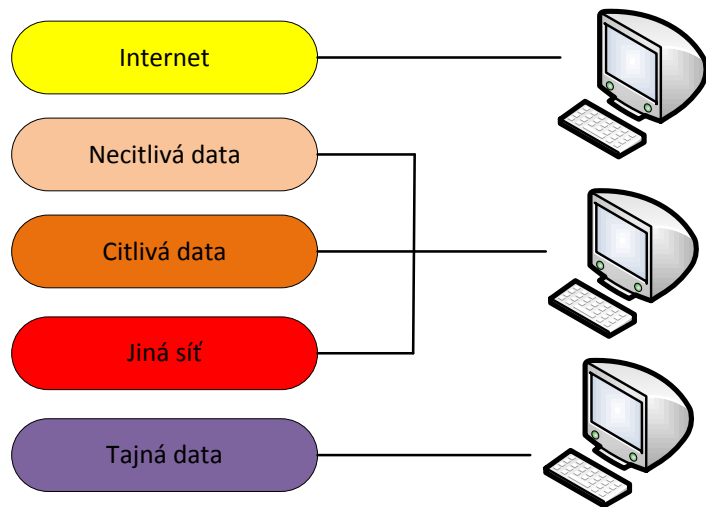
- Zachovat oddělenost jednotlivých systémů
- Nepropojit

Představované řešení:

- **HP ProtectTools a HP SecureSolutions**



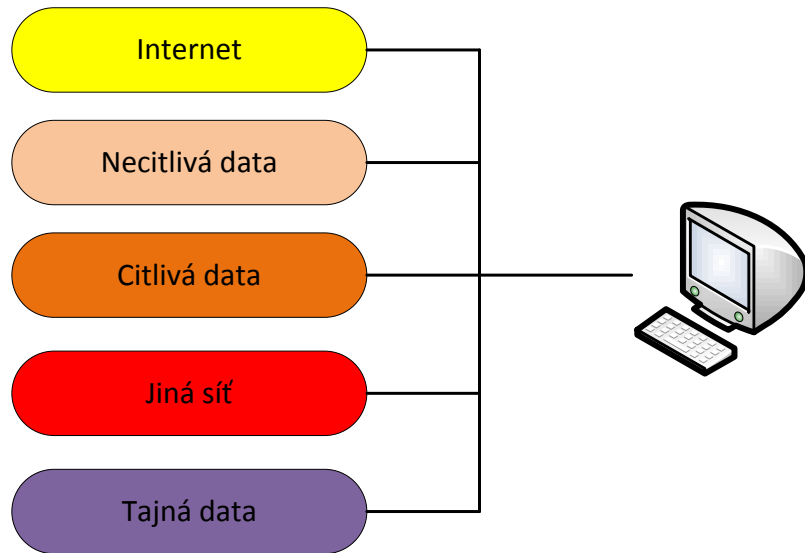
Problém přístupu k doménám s různou bezpečnostní klasifikací



Stávající stav – sítě nejsou odděleny. Přístupy k tajným datům, Internetu a ostatním datům jsou řešeny různými fyzickými počítači. Pro každou doménu různá tiskárna atd.

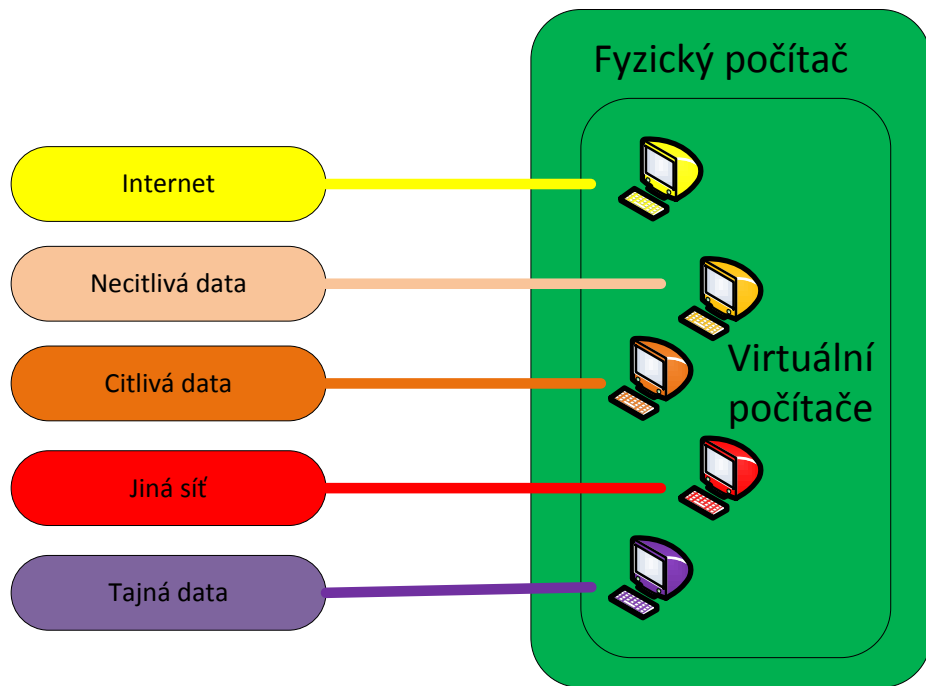
Termínem Tajná data jsou myšlena „klasifikovaná data ve smyslu zákona č. 412“

Problém přístupu k doménám s různou bezpečnostní klasifikací



Jeden fyzický počítač smíchává
dohromady data s různou
bezpečnostní klasifikací.
Nepřípustné řešení

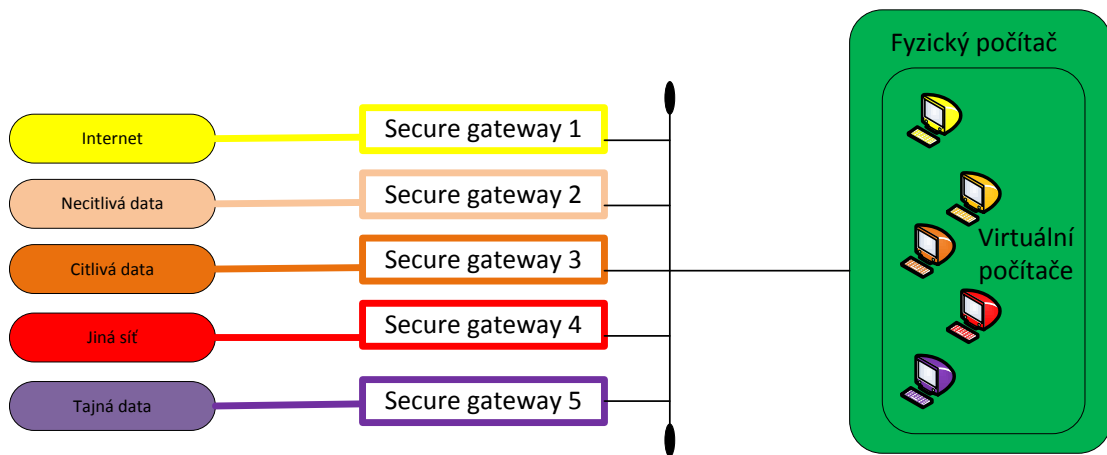
Problém přístupu k doménám s různou bezpečnostní klasifikací



Pokud bychom virtuální počítače přistupující k datům s různou bezpečnostní klasifikací udělali běžnými prostředky bez specializovaných bezpečnostních produktů pak ovšem nevyřešíme: **system přístupových práv podle rolí uživatele ani možnost kopírovat data mezi jednotlivými virtuálními stroji nebo do/z počítačových periférií.**

Problém přístupu k doménám s různou bezpečnostní klasifikací

HP ProtectTools a HP SecureSolutions



HP NetTop

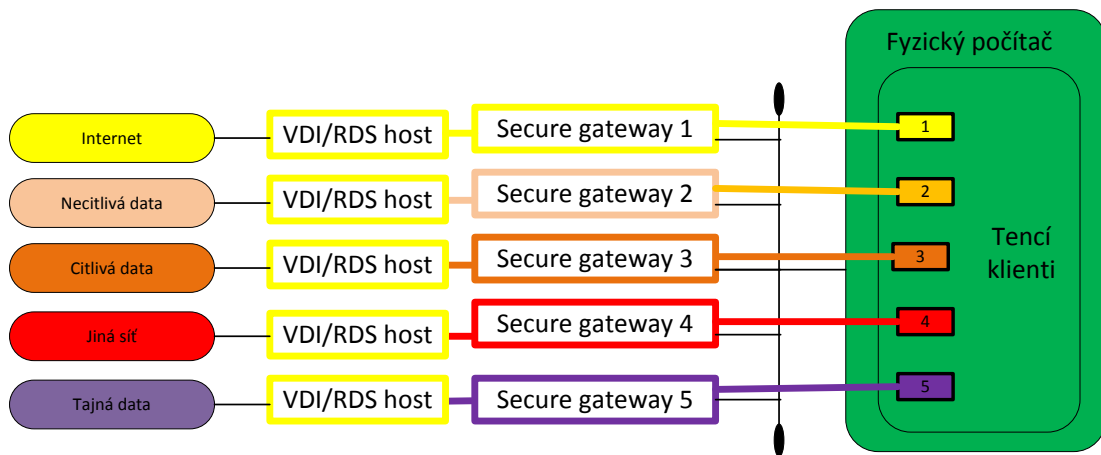
Virtuální počítače umístěné na fyzickém počítači. Mezi jednotlivými virtuálními počítači lze překlíkat, není ale možné mezi nimi přenášet data.

Data jsou fyzicky umístěná na uživatelské počítači. Důvěrnost informací je zajištěna ssl.

Nevýhodou jsou vyšší nároky na uživatelskou pracovní stanici.

Problém přístupu k doménám s různou bezpečnostní klasifikací

HP ProtectTools a HP SecureSolutions



HP Client Virtualisation Access Solution

Na fyzickém počítači jsou umístěny tenčí klienti. Mezi jednotlivými tenkými klienty lze překlíkávat, není ale možné mezi nimi přenášet data.

Výhodou jsou běžné nároky na uživatelskou pracovní stanici. Data jsou fyzicky umístěna na konkrétním VDI/RDS serveru, ke kterému se uživatel pomocí tenkého klienta připojuje. Důvěrnost informací je zajištěna ssl.

HP ProtectTools a HP SecureSolutions

Řešení

Komunikace uvnitř domén a mezi doménami s různou bezpečnostní klasifikací

Integruje technologie HP a HP partnerů

Akreditovatelné řešení

Řešení založené na HP ProtectTools a HP SecureSolutions dosahuje hodnocení EAL 4+ a více a je dobrým základem pro certifikaci v zamích nasazení (NBÚ v ČR)

Opakovetelné

Instalační balíčky, dokumentace, licencovaný produkt

Podpora

HP produkt s plnou podporou HP jako dodavatele



HP ProtectTools a HP SecureSolutions

Portfolio I

Jméno produktu z rodiny HP ProtectTools HP SecureSolutions	Popis a použití produktu
HP Client Virtualisation Access Solution - CVAS	Bezpečný přístup k datům s různou bezpečnostní klasifikací pomocí tenkého klienta z jednoho místa.
Role Based Access - RBA	Předášení dat mezi jednotlivými tenkými klienty např.pomocí clipboardu pomocí RBA je omezené nebo zcela zakázané. Nastavování přístupových práv je založené na definování uživatelských rolí.
Multiple Network Access	Umožňuje uživatelům přístup k aplikacím a informacím ze sítí s různou úrovní bezpečnostní klasifikace z jediné uživatelské pracovní stanice aniž se naruší integrita a důvěrnost dat
Data Tunnel	Framework pro přenos dat z místa A do místa B. Jakým způsobem se oddělí A od B závisí na tom, jakého charakteru místa A a B v konkrétním případě jsou. Může jít o konptetní jednosměrnou komunikaci (dioda) nebo o oddělení za pomoci firewallů (WebServices) ap.

HP ProtectTools a HP SecureSolutions

Portfolio II

Jméno produktu z rodiny HP ProtectTools HP SecureSolutions	Popis a použití produktu
Authentication Services	Autentizační služby jako je logování přístupů, vícefaktorová autentizace, generování hesel podle nastavených algoritmů a heslových politik, logoff šetříče obrazovek ap.
Enterprise Device Access Manager	Centralizovaná kontrola zařízení, které mohou a nebo naopak nesmí být připojeny k pracovním stanicím. Nastavení může být vztaženo k rolím přiřazeným uživateli.
Email Release Manager	Centralizovaná bezpečnostní politika týkající se mailů v organizaci.
Trusted Audit	Umožňuje auditovat logy a data z různých zdrojů, jejich přenos do centralizovaného místa k dalším analýzám a archivaci. Umožňuje řešit integritu logových záznamů a dat pomocí elektronických podpisů a časových razítek



HP ProtectTools a HP SecureSolutions

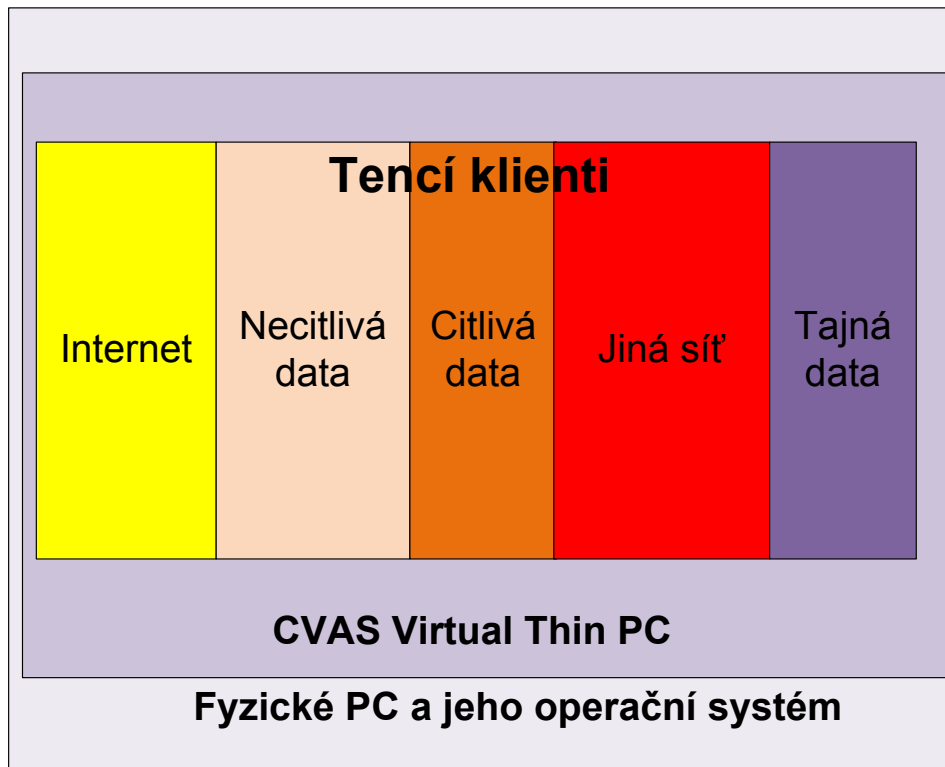
Portfolio III

Jméno produktu z rodiny HP ProtectTools HP SecureSolutions	Popis a použití produktu
Data Courier Data Gateways	Umožňuje uživatelům řízený a auditovaný přesun dat mezi doménami s různou úrovní bezpečnostní klasifikace podle centrálně nastavitelných pravidel. Celý proces je auditován. Data Couriers rozlišuje přenos souborů, bitstreamů, mailů a dat z clipboardů.
Secure Multiple Network Printing	Umožňuje bezpečné sdílení jedné soustavy tiskáren mezi doménami s různou úrovní bezpečnostní klasifikace.
One-way Transfer Gateway - dioda	End-to-end řešení pro jenosměrnou komunikaci. Dosažena certifikace na ITSEC E6 a Common Criteria EAL7
Collaboration	Komunikace mezi více organizacemi
NetTop	Jednoduché řešení pro přístup do více sítí a k více doménám z jednoho fyzického počítače. Metoda zabezpečení operačního systému.



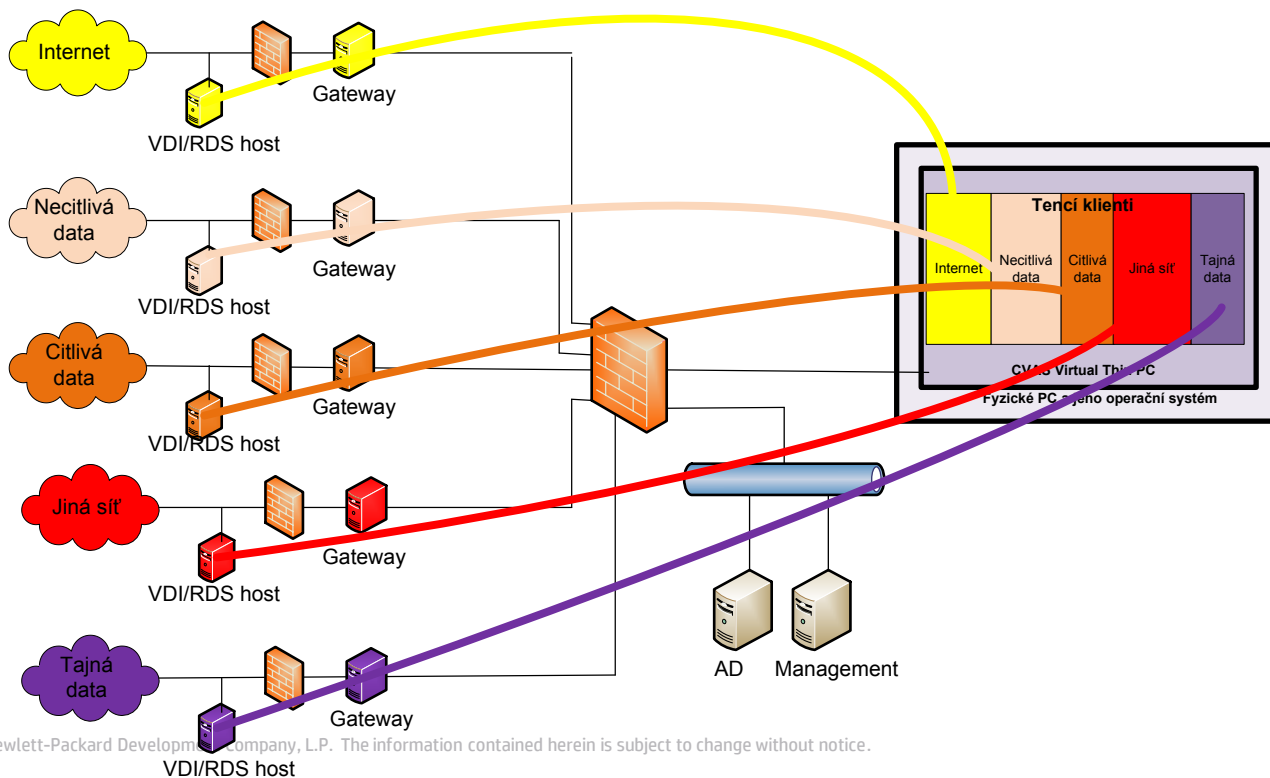
Architektura

Uživatelova pracovní stanice



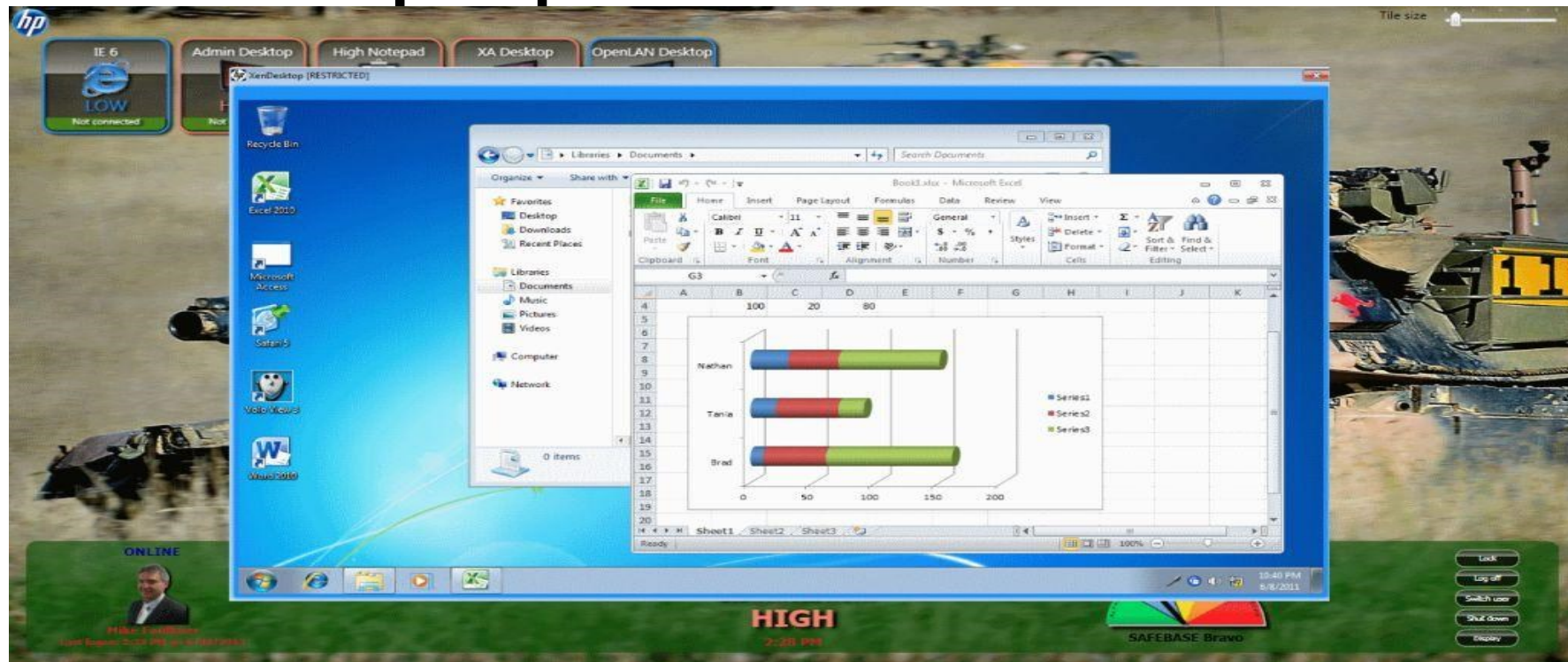
Architektura

Komunikace s jednotlivými doménami



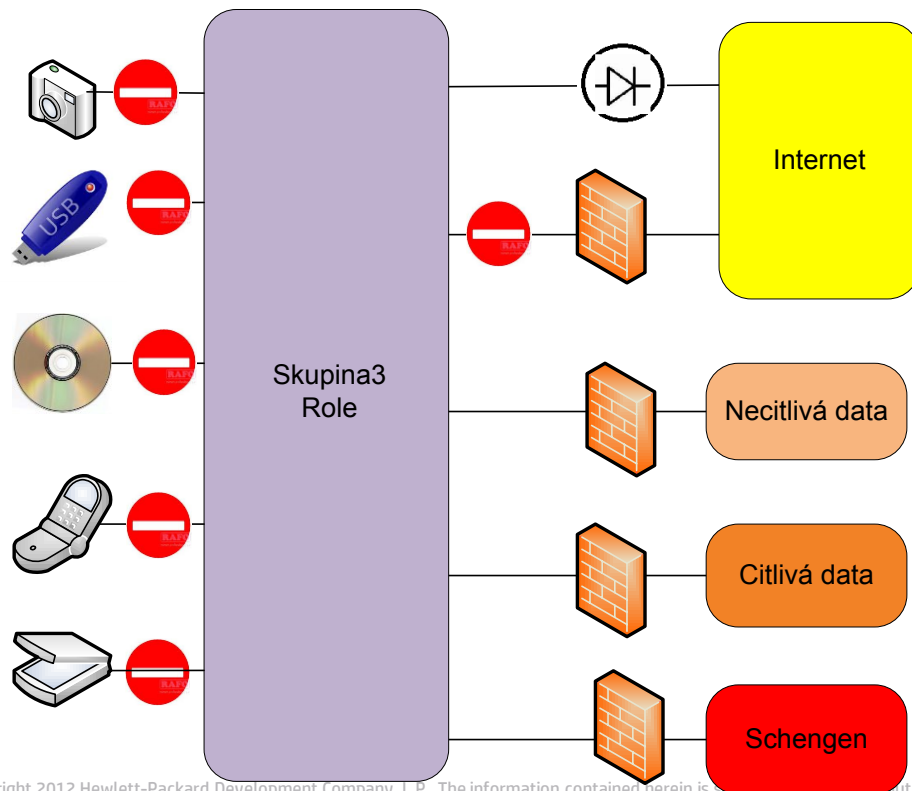
Co uživatel vidí na obrazovce

Virtual Desktop a aplikace



Zabezpečení uživatelské pracovní stanice

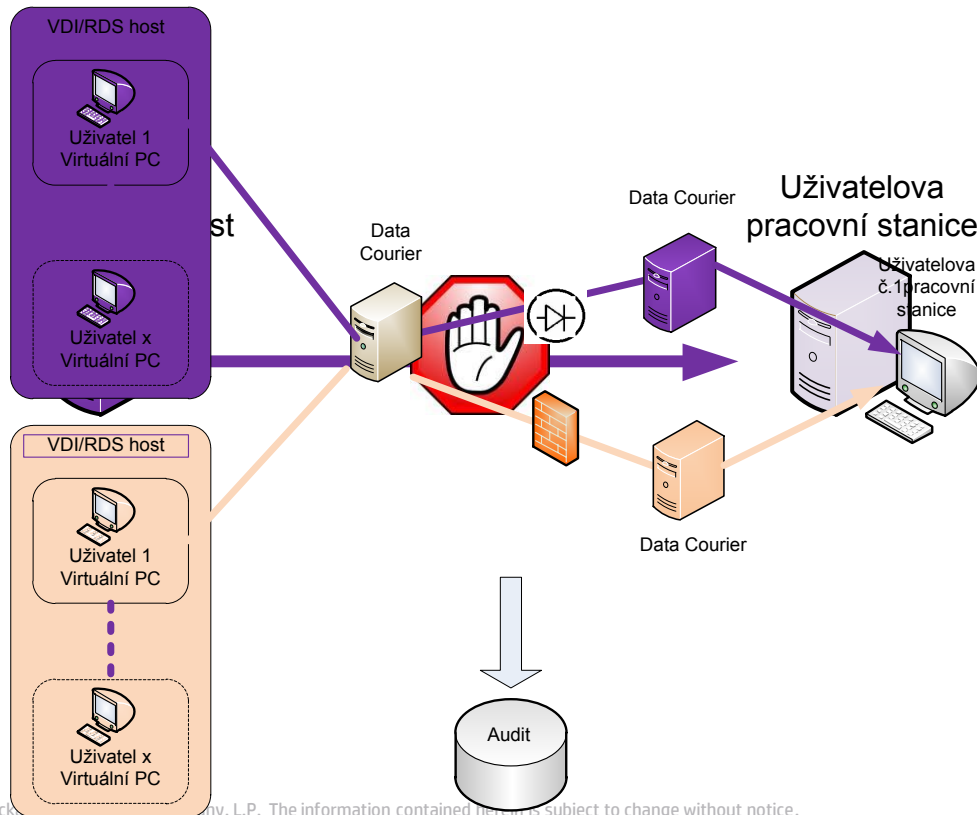
Enterprise Device Access Manager



K centrálnímu nastavení uživatelské pracovní stanice slouží HP Enterprise Device Access Manager. Nastavení se dá vztáhnout k přidělené roli – např. Skupina3. Podle toho bude mít uživatel např. zakázáno použití USB Flash a CD/DVD ap. Stejně tak může mít zablokovány některé síťové rozhraní. Stejně jako role přidělená aktuálně přihlášenému uživateli může ovlivnit povolení nebo zablokování zařízení a rozhraní na uživatelské pracovní stanici také přímo konkrétní HW.

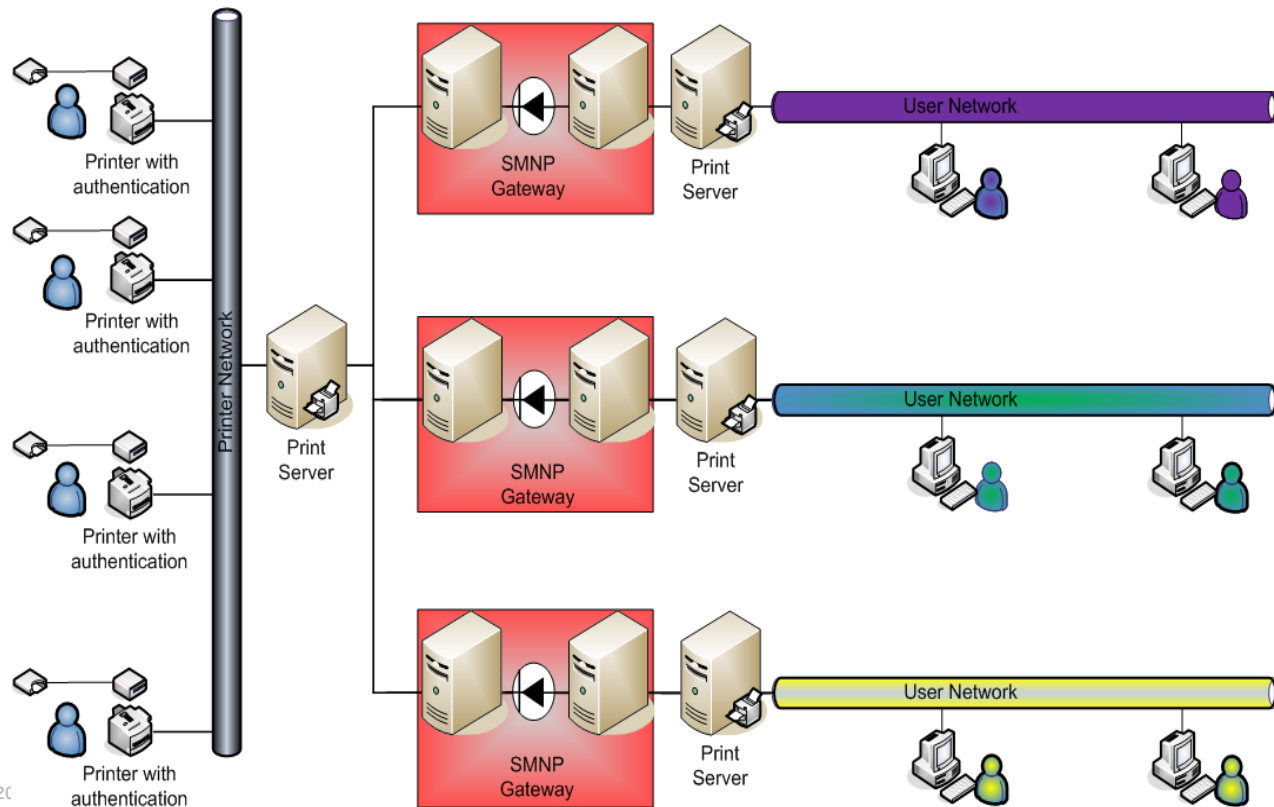
Kontrolované stahování dat - datový kurýr

Komunikace s jednotlivými doménami



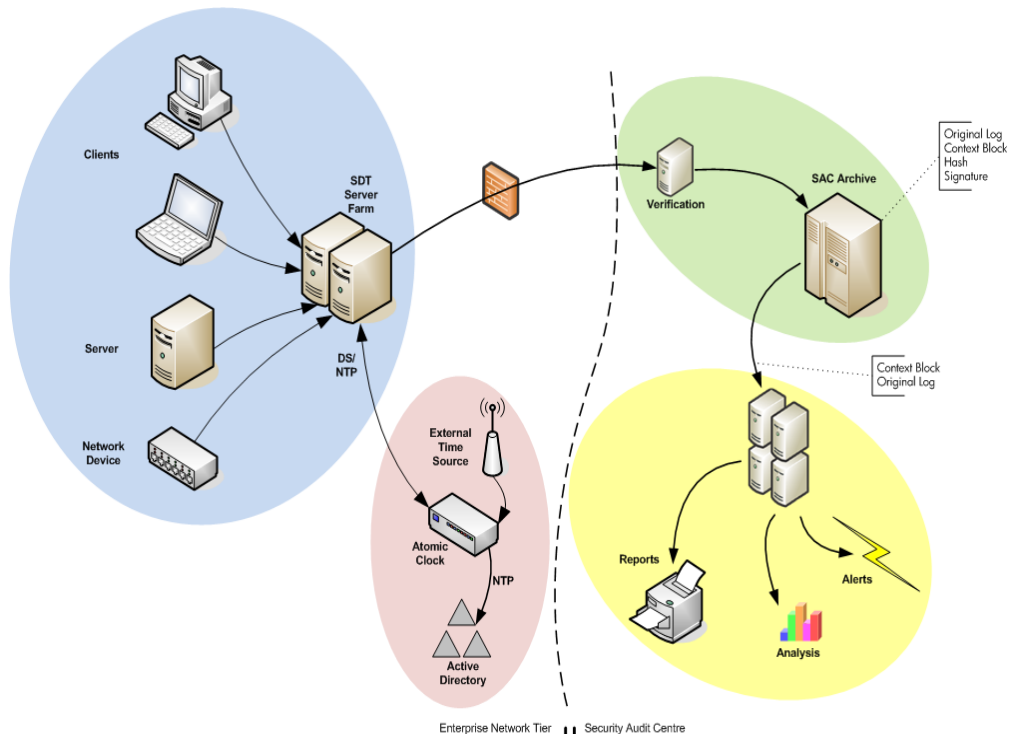
Další komponenty HP ProtectTools a HP SecureSolutions

Secure Multiple Network Printing



Další komponenty HP ProtectTools a HP SecureSolutions

Trusted Audit



Sbírá auditní záznamy z jednotlivých sítí a shromažďuje je na jediném místě – potravina pro SIEM (např. HP Arcsight)

HP ProtectTools a HP SecureSolutions poskytuje komplexní certifikované řešení problému komunikace mezi doménami s různou bezpečnostní klasifikací

Další informace na:

www.hp.com/services/protecttools

