UŽITNÝ VZOR

(11) Číslo dokumentu:
36 740
(13) Druh dokumentu: **U1**
(51) Int. Cl.:
H04L 69/22 (2022.01)

(19) ČESKÁ REPUBLIKA

ÚŘAD PRŮMYSLOVÉHO VLASTNICTVÍ

(21) Číslo přihlášky: **2022-40499**
(22) Přihlášeno: **18.11.2022**
(47) Zapsáno: **13.01.2023**

(73) Majitel:
Vysoké učení technické v Brně, Brno, Veveří, CZ

(72) Původce:
Ing. David Smékal, Dubicko, CZ
Ing. Zdeněk Martinásek, Ph.D., Brno, Bosonohy, CZ
Ing. Radek Fujdiak, Ph.D., Kuřim, CZ
prof. Ing. Jiří Mišurec, CSc., Brno, Jundrov, CZ

(74) Zástupce:
Kania, Sedlák, Smola, s.r.o., Mendlovo náměstí 907/1a, 603 00 Brno, Staré Brno

(54) Název užitného vzoru:
Hardwarová čistička síťového provozu

CZ 36740 U1

Úřad průmyslového vlastnictví v zápisném řízení nezjišťuje, zda předmět užitného vzoru splňuje podmínky způsobilosti k ochraně podle § 1 zák. č. 478/1992 Sb.

Hardwarová čistička síťového provozu

Oblast techniky

Technické řešení se týká hardwarové čističky síťového provozu obsahující FPGA síťovou kartu.

Dosavadní stav techniky

V současné době existující filtrační mechanismy využívají především statických záznamů nevhodných IP adres, které odpovídají nastaveným pravidlům firewallu v jádře dané technologie či platformy. Pravidla firewallu mohou být zpravidla stavová i nestavová a mohou ovlivňovat příchozí, odchozí i procházející IP datagramy. Pravidla slouží k ovlivňování průchodu paketů jádrem operačního systému a jsou zpracována procesorem daného počítačového systému.

Mechanismy jsou zpravidla tvořeny softwarovou implementací a rychlost filtrování závisí na použité platformě a výkonnosti procesoru, kde je systém nasazen. Samotný paketový přenos je pak realizován síťovou kartou, která pracuje na daném síťovém standardu a přenosová rychlost je dána právě touto technologií. V těchto řešeních se však zdaleka přenosová rychlost síťové karty nerovná rychlosti zpracování filtračních pravidel. Řádově se tato rychlost pohybuje v jednotkách Gb/s.

Na správu filtračních pravidel je zpravidla připojen systém detekce průniku, ve zkratce IDS, a systém prevence průniku. Ten při zjištění určité hrozby nebo incidentu analyzuje dané IP adresy a zahrne je do filtrační politiky. V záznamu IP adres jsou aktualizovány seznamy adres. Vložení nového záznamu může vyvolat i samotný uživatel.

Nevýhodou existujících řešení spočívá především v rychlosti filtrace, která zpravidla odpovídá výkonu procesoru serveru, na kterém daný filtr aplikován. Současná řešení sledují pouze hlavičky paketů a těžko se umí rozhodovat podle vyšších vrstev. Navíc nedokáží porozumět návaznosti jednotlivých paketů. Mnohdy existující řešení chaoticky nastavuje pravidla pro filtraci a tím je kladena velká pozornost při konfiguraci filtrů. Pro precizní zabezpečení potřebujeme mít povoleno právě to, co používáme a nic navíc. Mechanizmy se však liší podle implementačních návrhů.

Např. dostupné softwarové řešení v podobě aplikačního proxy serveru je nevýhodné pro uživatele v transparentnosti. Vždy je třeba u aplikací nastavit použití proxy serveru přičemž některé aplikace to nemusí umožňovat. Jde ale o softwarové řešení a musí se spoléhat na znalosti daných uživatelů. Také je třeba myslet na náročnost na výkon, protože každá služba potřebuje vlastní proxy. Tento problém předkládané řešení eliminuje, protože je daná služba filtrována již v síťovém uzlu představující FPGA síťová karta.

Cílem vynálezu je představit řešení, které výše uvedené nevýhody stavu techniky odstraní.

Podstata technického řešení

Výše zmíněné nedostatky odstraňuje do značné míry hardwarová čistička síťového provozu obsahující FPGA síťovou kartu, která obsahuje síťový modul určený pro příjem/odesílání paketů ze/do sítě a softwarový modul určený pro příjem/odesílání paketů do softwaru přes DMA kanály pomocí PCI sběrnice, jehož podstata spočívá v tom, že dále obsahuje filtrační modul určený pro hardwarovou implementaci vysokorychlostního filtrovaní datového provozu dle stanovených pravidel, a paměťový modul definující filtrační pravidla, tj. jaká komunikace bude filtrována.

Objasnění výkresů

Technické řešení bude dále přiblíženo pomocí obr. 1, který představuje FPGA síťovou kartu hardwarové čističky síťového provozu podle technického řešení.

Příklad uskutečnění technického řešení

Hardwarová čistička síťového provozu podle technického řešení obsahuje programovatelnou FPGA síťovou kartu, v blokovém schématu představenou na obr. 1, jež obsahuje

- síťový modul 1 určený pro příjem/odesílání paketů ze/do sítě,
- softwarový modul 2 určený pro příjem/odesílání paketů do softwaru přes DMA kanály pomocí PCI sběrnice,
- filtrační modul 3 určený pro hardwarovou implementaci vysokorychlostního filtrovaní datového provozu dle stanovených pravidel, a
- paměťový modul 4 definující filtrační pravidla, tj. jaká komunikace bude filtrována.

Síťové karty jsou zařízení zpracovávající data ze sítě. V daném případě se jedná o síťovou kartu, která obsahuje FPGA čip. FPGA je polovodičové zařízení, které se skládá ze tří hlavních částí, a to pole konfigurovatelných logických bloků (postavené z logických funkcí, jako např. AND, XOR a pamětí), programovatelných spojení a vstupně-výstupních bloků. Mezi výhody FPGA čipů patří přeprogramovatelnost jejich funkcí po výrobě a možnost vykonávat velký počet paralelních operací. Jelikož je tento FPGA čip, umístěný na síťové kartě, konfigurovatelný, je díky němu možné zpracovávat data a řídit datový tok uvnitř karty. Tím je možné filtrovat přenášené pakety.

Síťový modul 1 zajišťuje příjem a přenos síťových paketů. Síťový modul odesílá přijaté pakety do jádra aplikace uvnitř FPGA čipu přes datovou sběrnici. Již existující řešení, které využívá standardy síťové komunikace.

Softwarový modul 2 je ultrarychlý modul využívající přímý přístup do paměti, tzv. DMA („Direct Memory Access“), kanály s propustností 100 Gb/s na základě rozhraní PCIe. Komunikace plně odpovídá standardu PCIe sběrnice

Aplikační jádro je oblast čipu FPGA vyhrazená uživatelské aplikaci, která může těžit z NDK k zachycování paketů ze síťových rozhraní a odesílání dat do hostitelského CPU pomocí ultrarychlých přenosů DMA.

Filtrační modul 3 zahrnuje tzv. aplikační jádro, což je oblast čipu FPGA vyhrazená uživatelské aplikaci (filtračnímu modulu), která slouží k zachycování a dalšímu zpracování paketů ze síťových rozhraní a odesílání dat do CPU pomocí ultrarychlých přenosů DMA. Navržený filtrační modul umožňuje filtraci na základě komunikující IP adresy (statické i dynamické záznamy filtrovaných IP adres) a filtraci na základě dané služby (port služby, transportní protokol) s napojením na systém detekce průniku (IDS) a systém prevence průniku, definice IP adres verze 4 nebo 6 a mechanismus černé listiny, tj. seznam obsahující zakázané IP adresy, nebo bílé listiny, tj. seznam přístupu legitimních IP adres.

Paměťový modul 4 zahrnuje definici pravidel pro filtrování komunikace. Pravidla jsou filtračnímu modulu zadávány uživatelem prostřednictvím uživatelského skriptu.

Hardwarová část implementace čističky síťového provozu na síťové kartě s FPGA čipem využívá framework NDK („Network Development Kit“). Framework NDK zajišťuje komunikaci mezi

hardwarovou části běžící na FPGA čipu a softwarovou částí NDK obsahující řadiče, knihovny, nástroje, DMA („Direct Memory Access“) moduly a má přístup k hardwarovým registrům. Tato část umožňuje předávání dat mezi hardwarem a softwarem a současně umožňuje kontrolu a ovládání filtrační aplikace v aplikačním jádře FPGA z hostitelského počítače.

Hlavním benefitem představeného řešení je filtrace aplikovaná přímo na síťové kartě. Díky využití technologie FPGA a databází pravidel implementovaných přímo v aplikačním jádru na síťové kartě je filtrace velmi rychlá. Nedochází k žádnému zpoždění paketového přenosu. Přijatá data, která mohou přicházet ze síťového rozhraní nebo ze softwaru, jsou zpracována uvnitř vysokorychlostní síťové karty v reálném čase. Podle nastavených uživatelských pravidel jsou síťová data dále zpracována. Mohou být buď zpracována beze změn, zahozena nebo přeposlána na jiné rozhraní.

Hlavní použití se nabízí na vysokorychlostním uzlu síťového provozu, kde je potřeba odfiltrovat datovou komunikaci. Filtrační mechanizmus hardwarové čističky dokáže zpracovávat data do rychlosti 100 Gb/s. Na základě shody nalezených IP hlaviček lze pakety filtrovat dle stanovených pravidel. Konfigurace filtračního mechanizmu se nastavuje pomocí uživatelských filtračních pravidel pomocí skriptu.

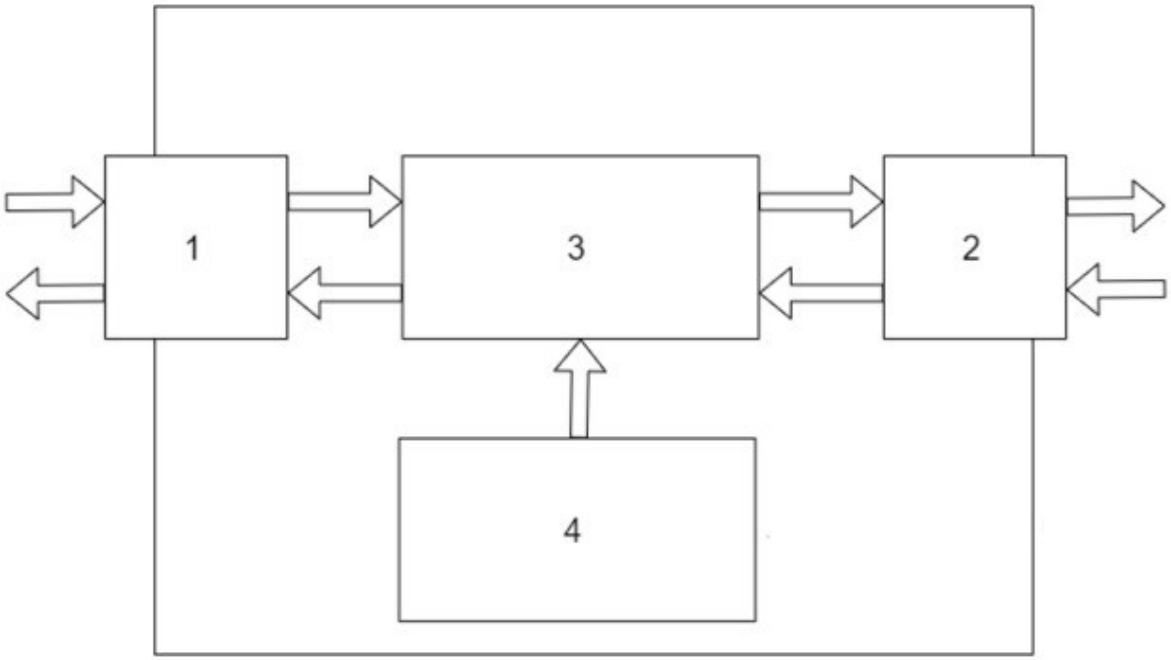
Programování a konfigurace filtračního aplikačního jádra na síťové kartě s FPGA čipem lze prostřednictvím programovacího jazyka VHDL a jazyka C.

Nasazení hardwarové implementace čističky provozu na vhodnou síťovou kartu s FPGA čipem lze pomocí IP bloku dané technologie.

NÁROKY NA OCHRANU

1. Hardwarová čistička síťového provozu obsahující FPGA síťovou kartu, která obsahuje síťový modul (1) určený pro příjem/odesílání paketů ze/do sítě a softwarový modul (2) určený pro příjem/odesílání paketů do softwaru přes DMA kanály pomocí PCI sběrnice, **vyznačující se tím**, že dále obsahuje filtrační modul (3) určený pro hardwarovou implementaci vysokorychlostní filtrace datového provozu dle stanovených pravidel, a paměťový modul (4) definující filtrační pravidla.

1 výkres



Obr. 1