

PATENTOVÝ SPIS

(11) Číslo dokumentu:

300 943

(19)
ČESKÁ
REPUBLIKA



ÚŘAD
PRŮMYSLOVÉHO
VLASTNICTVÍ

(21) Číslo přihlášky: **2002-3010**
(22) Přihlášeno: **06.09.2002**
(40) Zveřejněno: **14.04.2004**
(Věstník č. 4/2004)
(47) Uděleno: **17.08.2009**
(24) Oznámení o udělení ve Věstníku: **23.09.2009**
(Věstník č. 38/2009)

(13) Druh dokumentu: **B6**

(51) Int. Cl.:

G06F 13/00 (2006.01)

H04L 12/00 (2006.01)

(56) Relevantní dokumenty:

US 6170012; US 6026502; DE 19838253; CA 2432589; US 2002032755.

(73) Majitel patentu:

A && L SOFT s.r.o., Praha, CZ

(72) Původce:

Procháska Aleš Ing., Praha, CZ

(74) Zástupce:

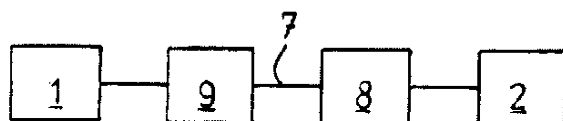
Ing. Ladislav Vaněk, Ortenovo nám. 6, Praha 7, 17000

(54) Název vynálezu:

**Způsob komunikace mezi sítěmi a propojení sítí
k jeho provedení**

(57) Anotace:

Způsob podle vynálezu spočívá v tom, že se datové spojení ze síťového zařízení umístěného v první síti (1) na výstupu z této první sítě (1) zakončí, přičemž se z "front" serveru (9) předá informace o nově ustaveném datovém spojení "back" serveru (8), jehož programový prostředek prověří oprávněnost tohoto datového spojení. Při oprávněnosti ustaveného datového spojení iniciuje "back" server (8) datové spojení se síťovým zařízením, umístěným v alespoň jedné další síti (2, 3, 4) a předává se mu datový obsah. Datový obsah v opačném směru se předává přes "back" server (8) na "front" server (9) a dále síťovému zařízení v první síti (1). Propojení sítí spočívá v tom, že má nekompatibilní člen (7) s protokolem rozdílným od standardních síťových protokolů v síti (1, 2, 3, 4), vložený mezi "front" server (9), připojený k první síti (1), a "back" server (8), připojený k alespoň jedné další síti (2, 3, 4).



CZ 300943 B6

Způsob komunikace mezi sítěmi a propojení sítí k jeho provedení

Oblast techniky

Vynález se týká způsobu komunikace mezi sítěmi, pomocí kterého se navzájem mezi sítěmi převádějí datová spojení a alespoň jedna síť se zabezpečuje proti zakázanému vstupu. Vynález se dále týká propojení sítí k provedení způsobu.

Dosavadní stav techniky

V současné době je zabezpečení dvou, případně více propojených sítí založeno na použití firewallu, který filtruje provoz mezi dvěma, případně více sítěmi a rozhoduje, která data a v jakých směrech smějí procházet z jedné sítě do druhé. Firewally jsou určeny především pro paketové protokoly, jako jsou v dnešní době nejpoužívanější protokoly TCP/IP. Způsob zabezpečení pomocí firewallu je v takových případech označován jako filtrování paketů.

Firewall je z hlediska logické struktury sítě transparentní člen pracující na nízké úrovni, který se fyzicky chová jako směrovač (router). Spolu komunikující síťová zařízení umístěná v různých sítích navazují spojení, v prostředí TCP/IP sítí zpravidla protokolem TCP respektive nad ním postaveným aplikačním protokolem, které transparentně prochází přes firewall a tudíž koncové body spojení jsou právě tato komunikující síťová zařízení.

Toto zabezpečení propojení dvou, případně více sítí, například připojení podnikové LAN na internet, má následující nevýhody:

- chyba v implementaci firewallu může umožnit útočníkovi nežádoucí průnik z jedné sítě do druhé,
- chyba v implementaci firewallu může umožnit útočníkovi manipulaci s konfigurací firewallu spolu s následným průnikem do chráněné sítě,
- chybná (nedostatečná) konfigurace firewallu může umožnit útočníkovi nežádoucí průnik z jedné sítě do druhé,
- nedostatečné zabezpečení firewallu samotného lze zneužít k útoku zevnitř z chráněné sítě, například za účelem umožnění průniku zvenčí, vynesení dat atd.

Firewall založený na filtrování paketů nemůže principiálně zabránit útokům spočívajícím ve zneužití bezpečnostních slabin síťových zařízení, a to ať z hlediska hardware nebo software, se kterými smí útočník legálně navázat komunikaci.

Podstata vynálezu

Úkolem vynálezu je vytvořit způsob komunikace mezi sítěmi a propojení sítí k jeho provedení, které nemají shora uvedené nevýhody stávajícího stavu techniky, nebo je alespoň minimalizují.

Způsob komunikace mezi sítěmi spočívá podle vynálezu v tom, že se datové spojení ze síťového zařízení umístěného v první síti na výstupu z první sítě přeruší, přičemž se z front serveru předá informace o nově ustaveném datovém spojení back serveru, jehož programový prostředek prověří oprávněnost tohoto datového spojení. Při oprávněnosti ustaveného datového spojení iniciuje back server datové spojení se síťovým zařízením umístěným v alespoň jedné další síti a předává mu datový obsah. Datový obsah v opačném směru se předává analogicky přes back server na front server a dále síťovému zařízení v síti.

Propojení sítě spočívá podle vynálezu v tom, že, a nekompatibilní člen s protokolem rozdílným od standardních síťových protokolů v síti, vložený mezi back server připojený k první síti a front server připojený k alespoň jedné další síti. Softwarové vybavení back serveru spravuje a řídí konfiguraci bezpečnostního systému, realizuje se síťovým prostředím nekompatibilní komunikační protokol pro komunikaci s front serverem a po nekompatibilním členu ovládá front server. Front server implementuje protilehlou část komunikačního protokolu a svoji činnost odvozuje od příkazů přijatých od back serveru. Back server instruuje front server, které příchozí spojení smí akceptovat a předávat na back server. Front server akceptuje povolená příchozí spojení a aplikační datový obsah předává spolu s informací o kategorii spojení back serveru. Back server podle kategorie spojení zvolí skutečné cílové zařízení, naváže s ním spojení a předává datový obsah od front serveru. Opačný datový tok je směřován analogicky s tím rozdílem, že potřebná spojení jsou již navázána.

V rozsahu vynálezu spočívá rovněž možnost pro zajištění proti útoku zevnitř další sítě propojení sítí rozšířit o další front server vložený mezi back server a další síť.

Přitom je výhodné, když protokol nekompatibilního členu má charakteristiku point-to-point.

Způsob a propojení sítí podle vynálezu přináší odstranění, nebo alespoň minimalizaci shora uvedených bezpečnostních nedostatků firewallů. Výhody způsobu a propojení sítí podle vynálezu spočívají zejména v tom, že:

- implementace front serveru a back serveru jednoduchá, a tudíž při ovládnutí front serveru, je velmi přístupného z první sítě, je minimalizováno riziko zneužití případné chyby v implementaci,
- ani vlivem chyby v implementaci front serveru nelze manipulovat s konfigurací, protože je spravována útočníkovi nepřístupným back serverem, který neimplementuje rozhraní pro její změny z front serveru první sítě,
- konfigurace zabezpečení na úrovni aplikačních spojení je řádově jednodušší, než konfigurace filtrovacích pravidel na úrovni jednotlivých paketů, tudíž je sníženo riziko mylné konfigurace bezpečnostního zařízení,
- nedostatečné zabezpečení front serveru, vedoucí k jeho úplnému ovládnutí útočníkem, nemožný průnik do další sítě, protože propojení obou sítí je realizováno nekompatibilním členem, který není standardně přístupný pro útočníkem použité síťové protokoly. Použití front serveru v obou sítích s back serverem uprostřed, umožňuje stejnou ochranu proti útoku z obou sítí.

Další výhodou způsobu a propojení sítí podle vynálezu je, že nejsou omezeny na žádnou konkrétní technologii, a to jak po stránce hardwaru (přenosových médií), tak i síťových protokolů a softwaru, a lze je, jednoduše bez dalších opatření, pro dosažení komplexního bezpečnostního systému kombinovat s dalšími prvky, které řeší jiné aspekty bezpečnosti, jako například s HTTP proxy, se zajištěním šifrování dat a autentizace přístupu pomocí SSL, se SOCKS proxy, s verifikací směřovaných aplikačních protokolů, samotným filtrováním paketů realizovaným za současného stavu techniky firewalů a podobně.

Přehled obrázků na výkrese

Další podrobnosti vynálezu jsou v následujícím objasněny pomocí výkresů na příkladech provedení. Na výkresech znázorňuje:

- obr. 1 propojení dvou sítí, z nichž druhá je chráněna před útokem z první sítě,
- obr. 2 propojení dvou sítí, z nichž každá je chráněna před útokem ze zbývajících sítí a samotný back server je chráněn před útokem z každé sítě,

obr. 3 propojení čtyř sítí, z nichž každá je chráněna před útoky z libovolné jiné sítě a samotný back server je chráněn před útokem z každé sítě.

5 Příklady provedení vynálezu

Na obr. 1 znázorněné propojení sítí 1, 2 propojuje první síť 1 a druhou síť 2. Sestává z front serveru 9, který je připojen k první síti 1, a z back serveru 8, který je připojen ke druhé síti 2. Mezi front serverem 9 a back serverem 8 je vložen nekompatibilní člen 7. Front server 9 i back server 8 jsou u tohoto příkladu provedení tvořeny počítačem s příslušným operačním systémem. Toto propojení umožňuje, že se datové spojení ze síťového zařízení umístěného v první síti 1 na výstupu z první sítě 1 zakončí, přičemž se z front serveru 9 předá informace o nově ustaveném datovém spojení back serveru 8, jehož programový prostředek prověří oprávněnost tohoto datového spojení. Při oprávněnosti ustaveného datového spojení iniciuje back server 8 datové spojení se síťovým zařízením umístěným ve druhé síti 2 a předává mu datový obsah. Datový obsah v opačném směru se předává analogicky přes back server 8 na front server 9 a dále síťovému zařízení v první síti 1.

Propojení první sítě 1 a druhé sítě 2, znázorněné na obr. 2 sestává ze dvou front serverů 9, tvořených počítači, z nichž první front server 9 je připojen k první síti 1 a druhý front server 9 je připojen ke druhé síti 2. Mezi oběma front servery 9 je zapojen back server 8, tvořený rovněž počítačem, přičemž mezi front servery 9 a back serverem 8 jsou vloženy nekompatibilní členy 7. Toto provedení umožňuje realizaci způsobu podle vynálezu také u příchozího datového spojení ze síťového zařízení umístěného v první síti 1, jak je popsáno v souvislosti s obr. 1, ale obdobně také u příchozího datového spojení ze síťového zařízení umístěného v druhé síti 2. Tím je první síť 1 chráněna proti útoku z druhé sítě 2 a back server 8 samotný je navíc na rozdíl od případu na obr. 1 chráněn proti útoku z druhé sítě 2.

Na obr. 3 je znázorněno propojení čtyř sítí 1, 2, 3, 4, které sestává ze čtyř front serverů 9, který jsou připojeny vždy jeden front server 9 k jedné síti 1, 2, 3, 4 a back serveru 8, který je zapojen mezi těmito front servery 9, přičemž mezi front servery 9 a back serverem 8 jsou vloženy nekompatibilní členy 7. Front servery 9 i back server 8 jsou i v tomto případě tvořeny počítači. Pomocí tohoto propojení je každá ze sítí 1, 2, 3, 4 chráněna před útoky z libovolné z těchto sítí 1, 2, 3, 4.

Způsob podle vynálezu lze v prostředí dnes nejběžněji používaných sítí TCP/IP s přenosovým médiem Ethernet realizovat pomocí back serveru 8 a front serverů 9, tvořenými běžnými počítači s vhodným operačním systémem (MS Windows, Linux a podobně) a nekompatibilním členem 7, tvořeným standardními nebo vysokorychlostními sériovými porty, nebo rozhraním SCSI (Small Computer System Interface), nebo rozhraním SCI (Scalable Coherent Interface), případně proprietárním propojovacím zařízením nekompatibilním s TCP/IP a Ethernetem a pomocí speciálního ho aplikačního softwarového vybavení realizujícího vlastní bezpečnostní funkce.

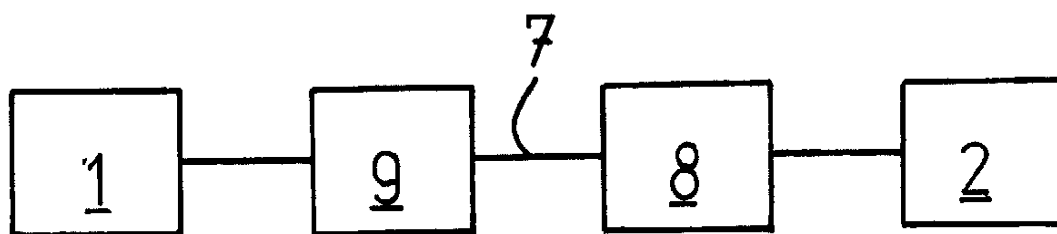
PATENTOVÉ NÁROKY

1. Způsob komunikace mezi sítěmi, pomocí kterého se navzájem mezi sítěmi (1, 2, 3, 4) převádějí datová spojení a alespoň jedna síť (1, 2, 3, 4) se zabezpečuje proti zakázanému vstupu, **v y z n a ě u j í c í s e t í m**, že se datové spojení ze síťového zařízení umístěného v první síti (1) na výstupu z této první sítě (1) zakončí, přičemž se z front serveru (9) předá informace o nově ustaveném datovém spojení back serveru (8), jehož programový prostředek prověří oprávněnost tohoto datového spojení, při oprávněnosti ustaveného datového spojení iniciuje back server (8)

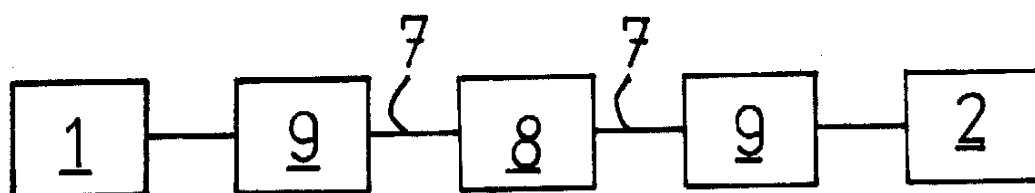
datové spojení se síťovým zařízením umístěným v alespoň jedné další síti (2, 3, 4) a předává se mu datový obsah, přičemž datový obsah v opačném směru se předává přes back server (8) na front server (9) a dále síťovému zařízení v první síti (1).

- 5 2. Propojení sítí k provedení způsobu komunikace mezi sítěmi podle nároku 1, **v y z n a č u - j í c í s e t í m**, že má nekompatibilní člen (7) s protokolem rozdílným od standardních síťových protokolů v síti (1, 2, 3, 4), vložený mezi front server (9), připojený k první síti (1), a back server (8), připojený k alespoň jedné další síti (2, 3, 4).
- 10 3. Propojení podle nároku 2, **v y z n a č u j í c í s e t í m**, že mezi back serverem (8) a další sítí (2, 3, 4) je vložen další front server (9).
- 15 4. Propojení podle nároku 2 nebo 3, **v y z n a č u j í c í s e t í m**, že protokol nekompatibilního členu (7) má charakteristiku, point-to-point.

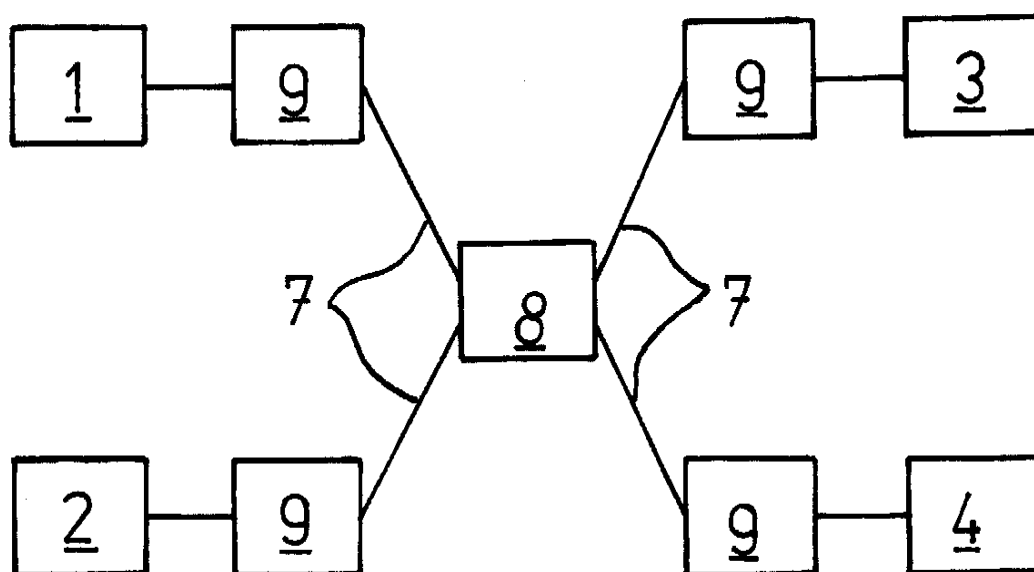
1 výkres



Obr. 1



Obr. 2



Obr. 3

 Konec dokumentu
