(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-518117
(P2005-518117A)
(43)公表日　平成17年6月16日(2005.6.16)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 12/46	H04L 12/46	E	5K030
H04L 12/66	H04L 12/66	B	5K033

審査請求 有　予備審査請求 有　（全 13 頁）

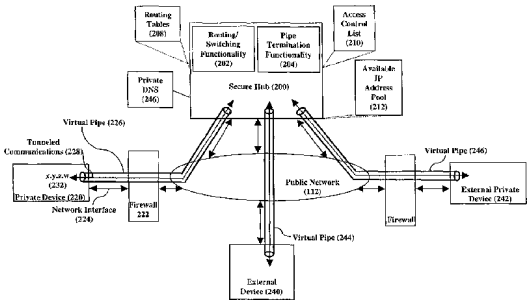
(21)出願番号	特願2003-568549 (P2003-568549)
(86)(22)出願日	平成15年1月15日 (2003.1.15)
(85)翻訳文提出日	平成16年7月15日 (2004.7.15)
(86)国際出願番号	PCT/US2003/001188
(87)国際公開番号	WO2003/069493
(87)国際公開日	平成15年8月21日 (2003.8.21)
(31)優先権主張番号	10/052,094
(32)優先日	平成14年1月18日 (2002.1.18)
(33)優先権主張国	米国(US)
(81)指定国	EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PT,SE,SI,SK,TR),CA,JP

(71)出願人　399047921
テルコーディア　テクノロジーズ　インコーポレイテッド
アメリカ合衆国　０８８５４－４１５７
ニュージャージー州　ピスカタウェイ　ワン　テルコーディア　ドライブ　５ジー１　１６
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　デイビッド　マープルズ
イギリス　エヌジー１８　４ジェイエイチ　マンスフィールド　ノッツ　バーチ　グローブ　５４

最終頁に続く

(54)【発明の名称】ファイアウォールとＮＡＴとを介してコネクションを開始する方法

(57)【要約】
ファイアウォール（２２２）およびＮＡＴを再コンフィギュアせずに、ファイアウォール（２２２）およびＮＡＴによって、パブリックネットワークから分離されたプライベートデバイス（２３０）にアクセスする。外部デバイス（２４０）へのアクセスを望むプライベートデバイスが、セキュアなハブ（２００）までのバーチャルプライベートパイプ（２２６）を確立し、ハブ（２００）は、バーチャルパイプをターミネートさせる機能と、このパイプとパブリックネットワーク（１１２）との間で通信をスイッチする機能を含む。このセキュアなハブは、２次ＩＰアドレスをプライベートデバイス／パイプに割り当て、これにより、ファイアウォール／ＮＡＴの背後のネットワークアピアランスをプライベートデバイスに提供する。外部デバイスは、通信を２次ＩＰアドレスにアドレスすることによってプライベートデバイスにアクセスし、この通信が、セキュアなハブにルーティングされ、このパイプを介してプライベートデバイスまでトンネリングされる。プライベートデバイスは、セキュアなハブによってエンフォースされるアクセスコントロー



【特許請求の範囲】
【請求項１】
第１デバイスがアクセスブロッキング装置によって第２デバイスから分離されており、前記第１デバイスに許可して前記第２デバイスと通信できるようにするハブによりパフォームされる方法であって、
前記第１デバイスからのバーチャルパイプをターミネートさせるステップと、
前記第１デバイスにＩＰアドレスを割り当て、該ＩＰアドレスを前記バーチャルパイプに関連付けするステップと、
前記第２デバイスによって発信され、前記ＩＰアドレスにアドレスされた通信を受信するステップと、
前記ＩＰアドレスにアドレスされた前記通信を前記バーチャルパイプにルーティングするステップと、
前記通信を前記バーチャルパイプを介して前記第１デバイスにトンネリングするステップと
を備えたことを特徴とする方法。
【請求項２】
請求項１に記載の方法において、
前記第１デバイスによってオリジネートされた第２通信を前記バーチャルパイプを介して受信するステップと、
前記第２通信を前記第１デバイスから前記第２デバイスにルーティングするステップとをさらに備えたことを特徴とする方法。
【請求項３】
請求項１に記載の方法において、前記通信を前記バーチャルパイプを介してトンネリングするステップの前に、前記通信を暗号化するステップをさらに備えたことを特徴とする方法。
【請求項４】
請求項１に記載の方法において、
複数の第２デバイスによってオリジネートされ、前記ＩＰアドレスにアドレスされた複数の通信を受信するステップと、
前記ＩＰアドレスにアドレスされた前記複数の通信を前記バーチャルパイプにルーティングするステップと、
前記複数の通信を前記バーチャルパイプを介して前記第１デバイスにトンネリングするステップと
をさらに備えたことを特徴とする方法。
【請求項５】
請求項１に記載の方法において、前記第１デバイスへのアクセスを制御するアクセスコントロールリストを確立し、該アクセスコントロールリストに基づき、前記第２デバイスが前記第１デバイスにアクセスする許可を有する場合にのみ、前記第２デバイスからの通信を前記第１デバイスにルーティングするステップをさらに備えたことを特徴とする方法。
【請求項６】
請求項１に記載の方法において、
前記第２デバイスからの第２バーチャルパイプをターミネートさせるステップと、
前記第２デバイスに第２ＩＰアドレスを割り当てるステップと、
前記第２デバイスからの通信を前記第２バーチャルパイプを介して受信するステップとをさらに備えたことを特徴とする方法。
【請求項７】
請求項６に記載の方法において、前記第１デバイスおよび前記第２デバイスに割り当てられた前記ＩＰアドレスは、プライベートＩＰアドレスであることを特徴とする方法。
【請求項８】

第１デバイスがアクセスブロッキング装置によって第２デバイスから分離されており、前記第１デバイスと前記第２デバイスとの間において通信を可能にするシステムであって、
セキュアなハブと、
前記第１デバイスと前記セキュアなハブとの間のバーチャルパイプと
を備え、
前記セキュアなハブは、ＩＰアドレスを前記第１デバイスに割り当てることができる、利用可能なＩＰアドレスプールと、前記割り当てられたＩＰアドレスとを前記バーチャルパイプに関連付けする手段と、前記第２デバイスからの前記第１デバイスにアドレスされた通信を前記バーチャルパイプにルーティングする手段と、前記通信を前記バーチャルパイプを介して前記第１デバイスにトンネリングする手段とを備えた
ことを特徴とするシステム。
【請求項９】
請求項８に記載のシステムにおいて、前記トンネリングする手段は、第２通信を前記バーチャルパイプを介して前記第１デバイスからトンネリングし、前記ルーティングする手段は、前記第２通信を前記第２デバイスにルーティングすることを特徴とするシステム。
【請求項１０】
請求項８に記載のシステムにおいて、前記第２デバイスと前記セキュアなハブとの間のバーチャルパイプをさらに備え、前記関連付けする手段は、前記利用可能なＩＰアドレスのプールからの第２ＩＰアドレスを前記第２バーチャルパイプに関連付けし、前記トンネリングする手段は、前記第２デバイスからの通信を前記第２バーチャルパイプを介してトンネリングすることを特徴とするシステム。
【請求項１１】
請求項８に記載のシステムにおいて、前記第１デバイスへのアクセスを制御するアクセスコントロールリストをさらに備え、前記アクセスコントロールリストに基づき、前記第２デバイスからの前記通信を前記第１デバイスにルーティングする手段は、前記第２デバイスが前記第１デバイスにアクセスする許可を有する場合にのみ、前記通信をルーティングすることを特徴とするシステム。
【請求項１２】
第２通信デバイスからパブリックネットワークを介して第１通信デバイスへの通信を可能にし、前記第１及び第２通信デバイスが少なくとも１つのセキュリティアクセスブロッキング装置によって分離されているシステムであって、
ルーティング機能およびスイッチング機能と、パイプターミネーション機能とを有し、前記パブリックネットワークとのインタフェースを有するセキュアなハブと、
通信をトンネリングするため前記セキュアなハブと前記第１通信デバイスとの間でバーチャルパイプを作成する手段と
を備え、
前記セキュアなハブは、前記第１通信デバイスにＩＰアドレスを割り当てる手段と、前記ＩＰアドレスを前記バーチャルパイプに関連付けする手段とをさらに備えた
ことを特徴とするシステム。
【請求項１３】
請求項１２に記載のシステムであって、前記第２通信デバイスから前記パブリックネットワークを介して前記セキュアなハブまでの通信を確立する手段をさらに備えたことを特徴とするシステム。
【請求項１４】
請求項１３に記載のシステムであって、前記第２通信デバイスからの通信を確立する手段は、第２バーチャルパイプを定義する手段を備えたことを特徴とするシステム。
【請求項１５】
請求項１２に記載のシステムであって、前記セキュアなハブは、アクセスコントロールリストを定義する手段を含み、前記ルーティング機能および前記スイッチング機能は、前

記アクセスコントロールリストによってアクセスが許可される場合にのみ、前記通信を前記第２通信デバイスから前記バーチャルパイプにルーティングすることを特徴とするシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、一般に、ファイアウォールとＮＡＴ（network address translator）とを介して通信することに関する。特に、本発明は、外部デバイスが、ファイアウォールおよびＮＡＴの背後にあるプライベートデバイスと、バーチャルプライベートパイプを介して、通信することができるようにするスイッチングシステム装置に関する。

【背景技術】

【０００２】

企業にとってもホームユーザにとっても、自らのローカルプライベートネットワークとパブリックネットワークとの間に、ファイアウォールおよび／またはＮＡＴを配置すること普通のことである。周知のとおり、ファイアウォールは、セキュリティに対処し、しかも、ローカルネットワークからパブリックネットワークに送信することができるトラフィックのタイプを規制するアクセスコントロールポリシーをエンフォース（enforce）するが、この規制対象のトラフィックのタイプとしては、パブリックネットワークからローカルネットワークにアクセスすることができるトラフィックのタイプの方が重要である。ＮＡＴによりある程度のセキュリティが提供され、その上、ＩＰアドレスの不足に直接対処することができるので、このＮＡＴによれば、プライベートネットワーク上のデバイスのセットは、単一のＩＰアドレスを使用して、パブリックネットワークとインタフェースすることができる。これら２つの技術は、アプリケーションは異なるが、同様の問題が生じる。すなわち、これら２つの技術によると、１つ又は複数のファイアウォール／ＮＡＴによって分離された２つのデバイス（例えば、コーポレート／パーソナルコンピュータ、サーバ、ネットワークアブライアンス等）が、オープンに通信することが、困難になる。

【０００３】

図１の例においては、デバイス１０６がパブリックネットワーク上に存在し、デバイス１０２が、ＮＡＴ１０４によってパブリックネットワーク１１２から分離されたプライベートホームネットワーク上に存在し、デバイス１１０が、ファイアウォール１０８によってパブリックネットワークから分離されたプライベートコーポレートネットワーク上に存在している。ファイアウォール１０８が外部通信を許可しているとの仮定の下では、デバイス１０２および１１０は、デバイス１０６との間で通信を開始することができる。ただし、ファイアウォール１０８が、デバイス１０６へアクセスできるように、最初に、再構成されるか、あるいはフォワーディングがＮＡＴ１０４上で最初に構成されて初めて、デバイス１０６は、デバイス１０２または１１０のいずれとも通信を容易に開始することができる。この状況は、仮にデバイス１０２と１１０が通信を望む場合には、幾分悪くなる。というのは、どちらのデバイスも、ファイアウォールおよび／またはＮＡＴが最初に再構成されて初めて、通信を開始することができるからである。

【０００４】

ファイアウォールおよびＮＡＴの再構成は、いくつかの理由から、前述した通信問題のソルューション（solution）にならない。第１に、再構成は管理プロセスであって、企業の承認を要することが多いから、ファイアウォールの再構成には時間がかかり、ＮＡＴにあっては、企業は、多くのユーザが有していないＩＰを理解する必要があって、ＮＡＴの再構成は困難である。第２に、再構成に必要な回数は、ファイアウォールまたはＮＡＴを介してアクセスしようとするデバイスの数が増えるにつれて、急速に増える。例えば、所望のピアツーピアコネクションは、全て、個別の再構成を要する。第３に、ファイアウォールおよびＮＡＴがパブリックアクセスに対してオープン化されるにつれて、セキュリティリスクが高くなる。

【発明の開示】

【発明が解決しようとする課題】
【０００５】
したがって、ファイアウォールおよびＮＡＴによって分離されたデバイスが、ファイアウォールおよびＮＡＴを再構成せずに通信することができ、かつセキュリティを低下させずに通信することができる、方法および装置を、提供するのが望ましく、この方法および装置により、前述した従来の技術の欠点その他の欠点を克服することができるのが望ましい。本発明によれば、セキュアなハブがパブリックネットワーク内に配置され、バーチャルなプライベートパイプをターミネート（terminate）させる機能が提供され、パブリックネットワークと、確立されたバーチャルプライベートパイプとの間での通信をスイッチする機能が提供される。
【課題を解決するための手段】
【０００６】
本発明の第１の実施形態によれば、ファイアウォールまたはＮＡＴによってパブリックネットワークから分離されたプライベートデバイスであって、外部デバイスへのアクセスを望むプライベートデバイスは、セキュアなハブに対するバーチャルプライベートパイプを確立する。このセキュアなハブは、２次パブリックＩＰアドレスをプライベートデバイス／パイプに割り当て関連付けする。このバーチャルパイプおよびＩＰアドレスは、このプライベートデバイス上に駐在するアプリケーションとの新規なインタフェースであり、このインタフェースを介して、外部デバイスへの通信を確立することができる。重要なことは、このセキュアなハブおよびバーチャルパイプは、ファイアウォール／ＮＡＴの背後のネットワークアピアランスをプライベートデバイスに供給する、ということである。そこで、外部デバイスは、２次ＩＰアドレスを使用して、通信にアドレスして、プライベートデバイスにアクセスすることができる。この通信は、セキュアなハブにルーティングされ、このセキュアなハブは、この２次ＩＰアドレスをパイプに関連付けし、この通信をプライベートデバイスまでトンネリングする。
【０００７】
本発明の第２実施形態によれば、当該プライベートデバイスは、外部デバイスへのアクセスを制限する。この場合、セキュアなハブは、前述したが、バーチャルパイプを確立することに加え、プライベートデバイスのためのアクセスコントロールリストを確立する。プライベートデバイスにアクセスするには、外部デバイスは、まず、セキュアなハブまでバーチャルパイプを確立することが好ましい。セキュアなハブは、アクセスコントロールリストを使用して、外部デバイスがプライベートデバイスにアクセスする許可を有するかどうかを、確立プロシージャの一部として、判定する。同様に、セキュアなハブは、プライベートデバイスにアドレスされた通信が外部デバイスから受信された時点で、アクセスが許可されるかどうかも判定することができる。アクセスが許可されたとの仮定の下において、通信は、外部デバイスからセキュアなハブまでトンネリングされ、このセキュアなハブは、この通信をプライベートデバイスまでルーティングし、トンネリングする。本発明に特有なことであるが、本発明は、ファイアウォール／ＮＡＴを再構成せずに、プライベートデバイスが、外部デバイスにセキュアにアクセスすることができる。
【発明を実施するための最良の形態】
【０００８】
図２は本発明に係るセキュアなハブ２００のブロック図であり、このハブ２００によれば、ファイアウォール／ＮＡＴ外のデバイス（以下、ファイアウォールというときは、ファイアウォール、ＮＡＴその他のデバイスまたは装置であって同様にアクセスを阻止するものを総称していう。）は、ファイアウォールを再構成せずに、そのファイアウォールの背後のデバイスと通信を開始し、そのデバイスに対してセキュアにアクセスすることができる。セキュアなハブ２００は、ファイアウォール外のパブリックネットワーク１１２上に駐在するスイッチングシステムである。このセキュアなハブ２００の目的は、ファイアウォール２２２の背後にあるプライベートデバイス２２０が、他のデバイスが通信をアドレスすることができるパブリックネットワーク上に、ネットワークアピアランスを作成す

ることができる点にあり、このネットワークアピアランスを作成することにより、ファイヤウォールの有する課題にアドレスせずに、セキュアなデバイスとの通信を開始することができ／このセキュアなデバイスへのアクセスを開始することができる点にある。

【０００９】

セキュアなハブ２００は、１つ以上のネットワークインタフェース２０６と、ルーティング／スイッチング機能２０２とを備え、ルーティング／スイッチング機能２０２により、セキュアなハブ２００は、１つ以上のネットワークインタフェース２０６と間でデータをスイッチングすることができる。加えて、セキュアなハブ２００は、「バーチャルプライベートネットワーク」／「パイプターミネーション」機能２０４を備え、この機能２０４と、スイッチング能力とにより、セキュアなハブ２００は、ターミネートされたバーチャルパイプと、ネットワークインタフェース２０６との間で、データをスイッチングすることができる。これらの能力により、プライベートデバイス２２０は、デバイス２４０および２４２のような外部デバイスをして、通信を開始させることができる。特に、プライベートデバイス２２０は、まず、自らのネットワークインタフェース２２４を介し、自らのファイアウォール２２２を経由して、セキュアなハブ２００まで、バーチャルプライベートパイプ２２６を確立する。ついで、セキュアなハブ２００は、例えば、このセキュアなハブ２００に割り当てられた利用可能なＩＰアドレスプール２１２の中から、２次ＩＰアドレス２３０を、プライベートデバイスに割り当て、この２次ＩＰアドレス２３０をバーチャルプライベートパイプ２２６に関連付けする。以下にさらに説明するが、２次ＩＰアドレス２３０は、アクセスが制限される、パブリックアドレスまたはプライベートアドレスとすることができる。プライベートデバイス２２０上に駐在するアプリケーションに対して、バーチャルプライベートパイプ２２６および２次ＩＰアドレス２３０は、新規なインタフェースであって、このインタフェースを介して、外部デバイスとの通信２２８を確立させることができる。例えば、アプリケーションは、ＩＰアドレス２３０を使用して通信をオリジネート（orignate）させることができ、この通信は、バーチャルプライベートパイプ２２６を介して、セキュアなハブ２００まで、トンネリングされ、ついで、セキュアなハブ２００のネットワークインタフェース２０６の１つを介して、パブリックネットワーク１１２にルーティングされる。

【００１０】

重要なことは、セキュアなハブ２００とバーチャルプライベートパイプ２２６が、ファイアウォール２２２の背後にあり外部デバイスが直接アクセス可能なプライベートデバイス２２０に、ネットワークアピアランスを供給する、ということである。例えば、ＩＰアドレス２３０がパブリックアドレスであるとの仮定の下では、外部デバイス２４０および２４２は、そのＩＰアドレス２３０に通信をアドレスすることにより、セキュアなハブ２００を介してプライベートデバイス２２０にアクセスすることができる。このようにアドレスされた通信は、セキュアなハブ２００にルーティングされ、このセキュアなハブ２００は、ＩＰアドレス２３０をバーチャルプライベートパイプ２２６２２６に関連付けし、このセキュアなハブ２００は、通信（２２８）を、バーチャルプライベートパイプ２２６を介し、ファイアウォールを経由して、プライベートデバイス２２０まで、ルーティング／トンネリングする。本発明の利点は、セキュアなハブ２００までバーチャルプライベートパイプ２２６を確立することにより、プライベートデバイス２２０は、ファイアウォールを再構成せずに、外部デバイスにセキュアなアクセスを提供することができる、点にある。

【００１１】

ユーザから要求があったとき、またはシステムがスタートアップされるとき等に、バーチャルプライベートパイプ２２６を確立することができる。バーチャルプライベートパイプ２２６については、ＰＰＴＰ（point-to-point tunnel protocol）またはＬ２ＴＰ（layer 2 tunnel protocol）などのプロトコルによりインプリメントすることができるが、本発明は、これらトンネリングプロトコルに特化した発明ではない。セキュリティ上の目的のため、バーチャルプライベートパイプ２２６を介してトンネリングされる通信２２８

を暗号化することができ、バーチャルプライベートパイプ２２６を、プライベートデバイス２２０において、次のようにしてコンフィギュア（configure）することができる。すなわち、バーチャルプライベートパイプ２２６が、特定のプライベートデバイス（又はこのプライベートデバイスのユーザ）を識別するが、プライベートネットワークに位置する任意のデバイスを識別しない、ことを保証するため、許可されていないオンワードルーティング（onward routing）により、コンフィギュアすることができる。加えて、セキュアなハブ２００は、パイプ確立の許可を得ているユーザのリストを保持することができ、かつパイプが確立されたとき、このリストに照らして、セキュアなデバイスを認証することができる。

【００１２】

バーチャルプライベートパイプ２２６を確立するプロシージャの一部として、セキュアなハブ２００は、前述したが、ＩＰアドレス２３０をプライベートデバイス２２０に割り当てることになり、かつアクセスコントロールリスト２１０についてプライベートデバイス２２０とネゴシエートすることもできる。１つのオプションとして、プライベートデバイス２２０は、任意の外部デバイスへのアクセスを許可することを決定することができる。この場合、アクセスコントロールリスト２１０は必要でないが、パブリックＩＰアドレスをバーチャルプライベートパイプ２２６に割り当てなければならない。そうであるから、セキュアなハブ２００は、利用可能なＩＰアドレスプール２１２から、利用可能なパブリックＩＰアドレスを獲得すること、ＩＰアドレス２３０がバーチャルプライベートパイプ２２６に関連付けられるように、ルーティングテーブル２０８をコンフィギュアすること、アプリケーションがＩＰアドレス２３０を使用することができるように、このＩＰアドレス２３０をセキュアなデバイスに通知すること、及び外部デバイスがセキュアなデバイスを見つけることができるように、ＤＮＳ（public domain name system）サーバ２４４を更新すること、を行うことになる。このシナリオにおいては、任意の外部デバイスは、すべての通信をそのパブリックアドレスにアドレスして、このセキュアなデバイスにアクセスすることができる。パブリックネットワーク１１２は、その通信を、セキュアなハブ２００にルーティングし、このセキュアなハブ２００は、そのアドレスをバーチャルプライベートパイプ２２６に関連付けし、この通信を、プライベートデバイス２２０までトンネリングする。ひとたびプライベートデバイス２２０がバーチャルプライベートパイプ２２６の使用を正常終了すると、プライベートデバイス２２０はバーチャルプライベートパイプ２２６をクローズし、セキュアなハブ２００は、そのＩＰアドレスをＩＰアドレスプール２１２に再割り当てする。オプションであるが、セキュアなハブ２００は、バーチャルプライベートパイプ２２６が、事前定義された期間において、アクティブであることを許可し、この期間の終了時において、バーチャルプライベートパイプ２２６を自動的にクローズし、ＩＰアドレスを再割り当てすることができる。

【００１３】

第２のオプションであるが、プライベートデバイス２２０は、外部デバイスの特定のセットへのアクセスを制限することを決定することができる。これを図３に示す。この場合、セキュアなハブ２００は、スイッチングシステムとしてアクトして、バーチャルプライベートパイプ２２６との間の通信をスイッチするだけでなく、ネットワークセキュリティも提供し、どの外部デバイスがプライベートデバイス２２０にアクセスするべきかを選択的に決定する。そうであるから、このセキュアなハブ２００は、プライベートデバイス２２０のアクセスコントロールリスト２１０を確立しコンフィギュアしなければならない。このアクセスコントロールリストは、例えば外部デバイスまたはユーザＩＤのリストを指定し、このアクセスコントロールリストを種々の方法で確立することができるが、これらはいずれも本発明に特有のものではない。セキュアなハブ２００は、例えば、Ｗｅｂベースのインタフェースまたは同様のインタフェースであってバーチャルプライベートパイプ２２６を経由しコネクションを介するものを使用して、アクセスコントロール情報に関するクエリを、プライベートデバイス２２０に対して行うことができる。セキュアなハブ２００が、ＩＰアドレスプール２１２からのプライベートＩＰアドレスを、このケースにお

いてプライベートデバイス２２０に割り当てることは、選択的なアクセスのインプリメントを容易にする上で、好ましいが、これは、パブリックアドレスの使用を排除するものではない。最後に、セキュアなハブ２００は、次のこと、すなわち、ＩＰアドレスがバーチャルプライベートパイプ２２６に関連付けられるように、自らのルーティングテーブル２０８をコンフィギュアすること、２次ＩＰアドレス２３０をプライベートデバイス２２０に通知すること、及び例えば外部デバイスがプライベートデバイス２２０を見つけることができるようにするため、プライベートＤＮＳサーバ２４６を更新すること、を行う。

【００１４】

この第２シナリオにおいては、プライベートデバイス２２０にアクセスするため、外部デバイス２４０または２４２が、まず、前述したとおり、セキュアなハブ２００までのバーチャルバーチャルプライベートパイプ２２６２４４または２４６をそれぞれ作成することが好ましい。再び、選択的なアクセスのインプリメントを容易にするため、プライベートＩＰアドレスは、この外部デバイスに割り当てられるべきであるが、これは、パブリックアドレスの使用を排除するものではない。１つのオプションであるが、この外部デバイスは、プライベートデバイス２２０と通信する意思を、パイプ確立プロシージャと認証プロシージャとの一部として、セキュアなハブ２００に明示する。

【００１５】

この要求に応答して、セキュアなハブ２００は、この外部デバイスがプライベートデバイス２２０のアクセスコントロールリスト２１０にリストされているかをベリファイし、仮にリストされている場合には、このデバイスからの将来の通信を、パイプ２２６を介して、プライベートデバイス２２０にルーティングすることができるという指示、を登録する。同様に、セキュアなハブ２００は、プライベートデバイス２２０にアドレスされた通信が、外部デバイスから受信された時点で、この外部デバイスがプライベートデバイス２２０にアクセスするかどうかを判定することができる。

【００１６】

上述したことと同様に、ひとたびセキュアなハブ２００が、外部デバイス２４０または２４２に関連するバーチャルパイプ２４４または２４６をコンフィギュアすると、この外部デバイス上のアプリケーションは、例えば、プライベートＤＮＳサーバ２４６を介してプライベートデバイス２２０に関連するＩＰアドレス２３２を知ることができる。そして、プライベートデバイス２２０にアドレスされた外部デバイス２４０または２４４からの後の通信は、セキュアなパイプ２４４または２４６を介してセキュアなハブ２００までトンネリングされ、このセキュアなハブは、ＩＰアドレス２３２をバーチャルプライベートパイプ２２６に関連付けし、この通信をプライベートデバイス２２０までトンネリングする。ひとたびプライベートデバイス２２０がこのセキュアなパイプの使用を正常終了すると、このセキュアなパイプをクローズし、セキュアなハブ２００は、ＩＰアドレス２３２をＩＰアドレスプール２１２に再割り振りする。オプションであるが、セキュアなハブ２００は、このセキュアなパイプが事前定義された期間中にのみアクティブであることを許可し、その期間の終了時において、このセキュアなパイプを自動的にクローズし、ＩＰアドレスを再割り振りすることができる。

【００１７】

以上説明した本発明の実施形態は例示のみを意図している。他の多数の実施形態は、本発明の趣旨および範囲を逸脱しない限り、当業者が提供することができる。

【図面の簡単な説明】

【００１８】

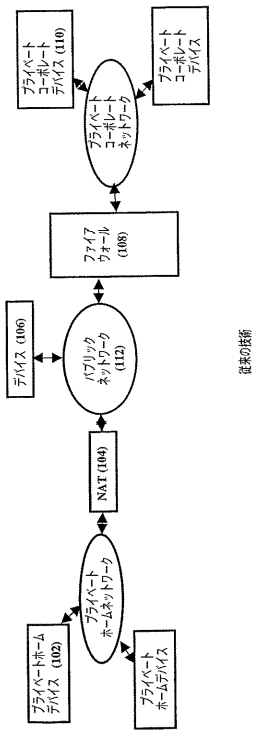
【図１】ＮＡＴおよびファイアウォールが、プライベートホームデバイスおよびプライベートコーポレートデバイスを、パブリックネットワークから分離するとの従来のアーキテクチャを示す図である。

【図２】第１の例示的な実施形態であって、プライベートデバイスがセキュアなハブまでセキュアなバーチャルプライベートパイプを作成し、このセキュアなハブが、プライベートデバイス／バーチャルパイプにパブリックＩＰアドレスを割り当て、関連付けし、これ

により、外部デバイスがアクセスすることができるパブリックネットワークアピアランスを、プライベートデバイスに提供する第１の例示的な実施形態を示す図である。

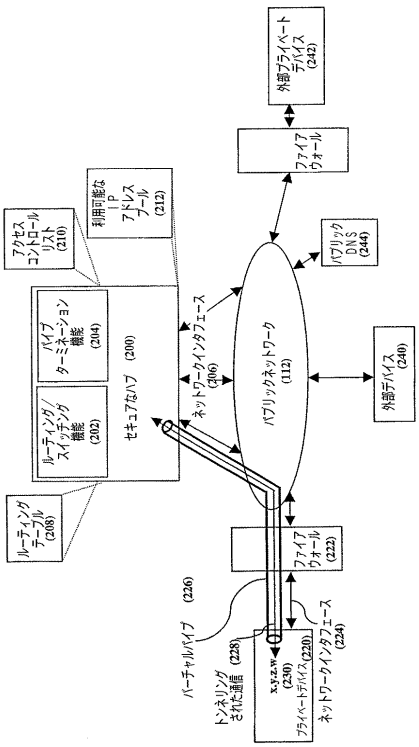
【図３】本発明の第２例示的な実施形態であって、プライベートデバイスがセキュアなハブまでのセキュアなバーチャルプライベートパイプを作成し、このセキュアなハブが、プライベートデバイスに対する制限されたアクセスをエンフォースし、この結果、外部デバイスがプライベートデバイスにアクセスできる前に、このセキュアなハブまでのセキュアなバーチャルプライベートパイプを確立する第２例示的な実施形態を示す図である。

【図１】

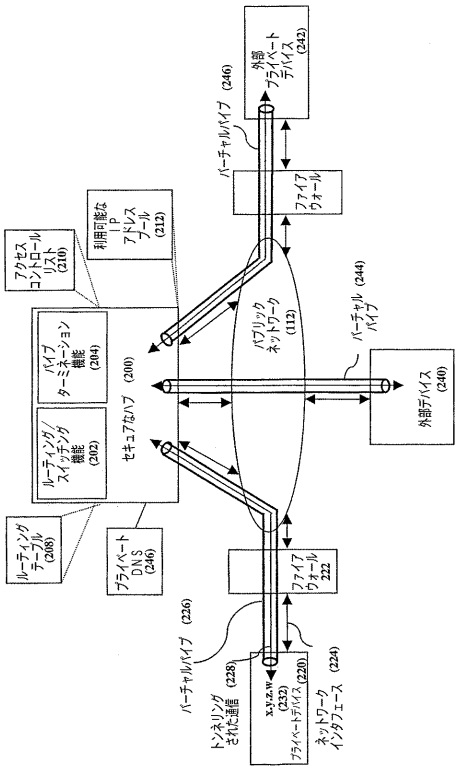


従来の技術

【図２】



【図３】


外部プライベートデバイス (242)
バーチャルパイプ (246)
ファイアウォール
利用可能なIPアドレスプール (212)
アクセスコントロールリスト (210)
パブリックネットワーク (112)
バーチャルパイプ (244)
パイプターミネーション機能 (204)
ルーティング/スイッチング機能 (202)
セキュアなVPN (200)
外部デバイス (240)
ルーティングテーブル (206)
プライベートDNS (246)
ファイアウォール 222
バーチャルパイプ (226)
トンネリングされた通信 (228)
X.25/X.3PAD (232)
プライベートデバイス (220)
ネットワークインタフェース (224)

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/01188

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F 15/16
US CL : 709/227, 222
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 709/227, 222

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
http://www1.ipdl.jpo.go.jp/PA1/cgi-bin/PA1INIT?996697333278

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y,P	US 2002/0152373 A1 (SUN et al) 17 October 2002 (17.10.2002), see entire document, especially page 1 paragraph 9, page 2 paragraph 13, page 3 paragraphs 39-40, page 4 paragraph 45 and paragraph 47 and page 7 paragraph 69)	1-15
Y	JP 2001339428 A (NAITO KATSUMI) 7 December 2001 (07.12.2001), see entire document, especially page 1 paraphraph 10	1-15
A	US 2002/0184316 A1 (THOMAS et al) 05 December 2002 (05.12.2002), see entire document	1-15
A	US 2002/0169980 A1 (BROWNELL) 14 November 2002 (14.11.2002), see entire document	1-15

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
03 April 2003 (03.04.2003)	24 APR 2003
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Ayaz sheikh Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

PCT/US03/01188

Continuation of B. FIELDS SEARCHED Item 3:
EAST
firewall, NAT, hub, switch, router, bridge, routing , terminating , virtual, logical, pipe, tunnel, channel, connection, ip address...

フロントページの続き

(72)発明者　スタンレー　エル．モイヤー
アメリカ合衆国　０７９４５　ニュージャージー州　メンドハン　カーロール　ドライブ　３
(72)発明者　クリスチャン　ウイティマ
アメリカ合衆国　９８００４　ワシントン州　クライド　ヒル　ノースイースト　３２　ストリート　９６４５

Ｆターム(参考) 5K030 GA15 HA08 HC01 HD03 HD07 HD09 LB02 LB05
5K033 AA08 CB01 CB06 CB08 DA06 DB12 DB17 DB18 EC04

【要約の続き】
ルリストを介してアクセスを制限することもできる。