(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6182397号
(P6182397)
(45)発行日　平成29年8月16日(2017.8.16)　(24)登録日　平成29年7月28日(2017.7.28)

(51)Int.Cl.　　F I
H04L 12/66 (2006.01)　　H04L 12/66　B
H04L 12/70 (2013.01)　　H04L 12/70　D

請求項の数 6　(全 18 頁)

(21)出願番号　特願2013-182353(P2013-182353)
(22)出願日　平成25年9月3日(2013.9.3)
(65)公開番号　特開2015-50698(P2015-50698A)
(43)公開日　平成27年3月16日(2015.3.16)
審査請求日　平成28年7月21日(2016.7.21)

(73)特許権者　000005290
古河電気工業株式会社
東京都千代田区丸の内二丁目２番３号
(73)特許権者　505173245
古河ネットワークソリューション株式会社
神奈川県平塚市東八幡５丁目１番９号
(74)代理人　100130247
弁理士　江村　美彦
(74)代理人　100167863
弁理士　大久保　恵
(72)発明者　植木　健
神奈川県平塚市東八幡５丁目１番９号　古河ネットワークソリューション株式会社内

最終頁に続く

(54)【発明の名称】ネットワークシステム、ブランチルータ、および、その制御方法

(57)【特許請求の範囲】
【請求項１】
複数のブランチルータを有する１以上のグループと、これら１以上のグループを制御するゲートウェイとを有するネットワークシステムにおいて、
前記ゲートウェイは、
各グループを構成する複数の前記ブランチルータに対してＭＰＳＡ（Multi-point Security Association）情報を配布する配布手段を有し、
前記複数のブランチルータは、
前記配布手段によって配布された前記ＭＰＳＡ情報に基づいてトンネル経路に従って相互に暗号化通信を行う通信手段と、
他のブランチルータから届いたパケットに付与されている第１送信元アドレスと、このパケットを復号化することによって得られる第２送信元アドレスとを取得する取得手段と、
前記取得手段によって得られた前記第２送信元アドレスに基づいて経路情報テーブルを検索し、該当する経路情報が前記トンネル経路であり、かつ、前記トンネル経路の送信インタフェースがこのパケットを受信したインタフェースと一致するとともに、前記トンネル経路の終端アドレスが前記第１送信元アドレスと一致するか否かを判定する判定手段と、
前記判定手段によって否と判定された場合にはそのパケットを破棄する破棄手段と、を有する、

ことを特徴とするネットワークシステム。
【請求項２】
前記判定手段は、前記取得手段によって取得された前記第１送信元アドレスが、前記経路情報テーブルに前記トンネル経路の終端アドレスとして登録されているか否かを前記パケットが復号化される前に判定し、
前記破棄手段は、前記判定手段によって否と判定された場合にはそのパケットを破棄する、
ことを特徴とする請求項１に記載のネットワークシステム。
【請求項３】
前記破棄手段は、前記ブランチルータが所定のＭＰＳＡから受信したパケットが同一のＭＰＳＡへ送信される場合にはそのパケットを破棄することを特徴とする請求項１または２に記載のネットワークシステム。
【請求項４】
複数のブランチルータを有する１以上のグループと、これら１以上のグループを制御するゲートウェイとを有するネットワークシステムの制御方法において、
前記ゲートウェイは、
各グループを構成する複数の前記ブランチルータに対してＭＰＳＡ情報を配布する配布ステップを有し、
前記複数のブランチルータは、
前記配布ステップにおいて配布された前記ＭＰＳＡ情報に基づいてトンネル経路に従って相互に暗号化通信を行う通信ステップと、
他のブランチルータから届いたパケットに付与されている第１送信元アドレスと、このパケットを復号化することによって得られる第２送信元アドレスとを取得する取得ステップと、
前記取得ステップにおいて得られた前記第２送信元アドレスに基づいて経路情報テーブルを検索し、該当する経路情報が前記トンネル経路であり、かつ、前記トンネル経路の送信インタフェースがこのパケットを受信したインタフェースと前記トンネル経路の終端アドレスが前記第１送信元アドレスと一致するか否かを判定する判定ステップと、
前記判定ステップにおいて否と判定された場合にはそのパケットを破棄する破棄ステップと、を有する
ことを特徴とするネットワークシステムの制御方法。
【請求項５】
複数のブランチルータを有する１以上のグループと、これら１以上のグループを制御するとともに、各グループを構成する複数の前記ブランチルータに対してＭＰＳＡ情報を配布する配布手段を備えるゲートウェイとを有するネットワークシステムを構成する前記ブランチルータにおいて、
前記配布手段によって配布された前記ＭＰＳＡ情報に基づいてトンネル経路に従って相互に暗号化通信を行う通信手段と、
他のブランチルータから届いたパケットに付与されている第１送信元アドレスと、このパケットを復号化することによって得られる第２送信元アドレスとを取得する取得手段と、
前記取得手段によって得られた前記第２送信元アドレスに基づいて経路情報テーブルを検索し、該当する経路情報が前記トンネル経路であり、かつ、前記トンネル経路の送信インタフェースがこのパケットを受信したインタフェースと一致するとともに、前記トンネル経路の終端アドレスが前記第１送信元アドレスと一致するか否かを判定する判定手段と、
前記判定手段によって否と判定された場合にはそのパケットを破棄する破棄手段と、を有する、
ことを特徴とするブランチルータ。
【請求項６】

複数のブランチルータを有する１以上のグループと、これら１以上のグループを制御するとともに、各グループを構成する複数の前記ブランチルータに対してＭＰＳＡ情報を配布する配布ステップを備えるゲートウェイとを有するネットワークシステムを構成する前記ブランチルータの制御方法において、

前記配布ステップにおいて配布された前記ＭＰＳＡ情報に基づいてトンネル経路に従って相互に暗号化通信を行う通信ステップと、

他のブランチルータから届いたパケットに付与されている第１送信元アドレスと、このパケットを復号化することによって得られる第２送信元アドレスとを取得する取得ステップと、

前記取得ステップにおいて得られた前記第２送信元アドレスに基づいて経路情報テーブルを検索し、該当する経路情報が前記トンネル経路であり、かつ、前記トンネル経路の送信インタフェースがこのパケットを受信したインタフェースと一致するとともに、前記トンネル経路の終端アドレスが前記第１送信元アドレスと一致するか否かを判定する判定ステップと、

前記判定ステップによって否と判定された場合にはそのパケットを破棄する破棄ステップと、を有する、

ことを特徴とするブランチルータの制御方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ネットワークシステム、ブランチルータ、および、その制御方法に関するものである。

【背景技術】

【０００２】

ＶＰＮ（Virtual Private Network）通信においては、ネットワークのハブ（Hub）となるゲートウェイと、このゲートウェイに接続されたスポーク（Spoke）となる複数のブランチルータによって構成されるＨｕｂ－ａｎｄ－Ｓｐｏｋｅ型ＶＰＮネットワークシステムが存在する。

【０００３】

ところで、このようなＨｕｂ－ａｎｄ－Ｓｐｏｋｅ型ＶＰＮネットワークシステムでは、拠点間通信がゲートウェイを通過することから、例えば、ブランチルータ同士が隣接地にあってもゲートウェイが遠隔地にある場合には伝送遅延が大きくなる。また、全ての通信がゲートウェイを通過することから通信量が大きくなり、ゲートウェイの設備負荷が大きくなるという問題点がある。

【０００４】

そこで、非特許文献１に記載されているように、複数のブランチルータによってグループを構成し、各グループ内における拠点間通信は共通のグループ鍵によってブランチルータ間で直接通信を行い、グループ鍵は、ゲートウェイから各ブランチルータに配布する技術が存在する。

【先行技術文献】

【非特許文献】

【０００５】

【非特許文献１】スター型とメッシュ型のハイブリッドＩＰ－ＶＰＮアーキテクチャ、電子情報通信学会、信学技報ＮＳ２０１２－２０，Ｍａｙ／２０１２

【発明の概要】

【発明が解決しようとする課題】

【０００６】

ところで、非特許文献１に開示された技術では、グループを構成する拠点間通信では、複数のブランチルータで共用する単一のグループ鍵を用いたＳＡ（Security Association）であるＭＰＳＡ（Multi-point Security Association）を使用することから、正常なパ

ケットを盗聴され、宛先を他のブランチルータの宛先に書き換えて再送された場合には、その他のブランチルータが復号化したパケットが本来のブランチルータに転送されるため、リプレイ（再送）攻撃が可能になってしまうという問題点がある（以下、リダイレクトによるリプレイ攻撃と呼ぶこととする）。

【０００７】

本発明は、以上の点に鑑みてなされたものであり、グループ内の複数のブランチルータで共用する単一のグループ鍵を共用するネットワークシステムにおいて、リダイレクトによるリプレイ攻撃を防止することが可能なネットワークシステム、ブランチルータ、および、これらの制御方法を提供することを目的としている。

【課題を解決するための手段】

【０００８】

上記課題を解決するために、本発明は、複数のブランチルータを有する１以上のグループと、これら１以上のグループを制御するゲートウェイとを有するネットワークシステムにおいて、前記ゲートウェイは、各グループを構成する複数の前記ブランチルータに対してＭＰＳＡ情報を配布する配布手段を有し、前記複数のブランチルータは、前記配布手段によって配布された前記ＭＰＳＡ情報に基づいてトンネル経路に従って相互に暗号化通信を行う通信手段と、他のブランチルータから届いたパケットに付与されている第１送信元アドレスと、このパケットを復号化することによって得られる第２送信元アドレスとを取得する取得手段と、前記取得手段によって得られた前記第２送信元アドレスに基づいて経路情報テーブルを検索し、該当する経路情報が前記トンネル経路であり、かつ、前記トンネル経路の送信インタフェースがこのパケットを受信したインタフェースと一致するとともに、前記トンネル経路の終端アドレスが前記第１送信元アドレスと一致するか否かを判定する判定手段と、前記判定手段によって否と判定された場合にはそのパケットを破棄する破棄手段と、を有する、ことを特徴とする。

このような構成によれば、グループ内の複数のブランチルータで共用する単一のグループ鍵を共用するネットワークシステムにおいて、リダイレクトによるリプレイ攻撃を防止することが可能となる。

【０００９】

本発明の一側面は、前記判定手段は、前記取得手段によって取得された前記第１送信元アドレスが、前記経路情報テーブルに前記トンネル経路の終端アドレスとして登録されているか否かを前記パケットが復号化される前に判定し、前記破棄手段は、前記判定手段によって否と判定された場合にはそのパケットを破棄することを特徴とする。

このような構成によれば、パケットを復号化する前に、正当でないパケットを破棄するので、正当でないパケットに処理を費やすことを防止できる。

【００１０】

本発明の一側面は、前記破棄手段は、前記ブランチルータが所定のＭＰＳＡから受信したパケットが同一のＭＰＳＡへ送信される場合にはそのパケットを破棄することを特徴とする。

このような構成によれば、正当でないパケットを破棄するので、トラフィックの増加を抑制することができる。

【００１１】

また、本発明は、複数のブランチルータを有する１以上のグループと、これら１以上のグループを制御するゲートウェイとを有するネットワークシステムの制御方法において、前記ゲートウェイは、各グループを構成する複数の前記ブランチルータに対してＭＰＳＡ情報を配布する配布ステップを有し、前記複数のブランチルータは、前記配布ステップにおいて配布された前記ＭＰＳＡ情報に基づいてトンネル経路に従って相互に暗号化通信を行う通信ステップと、他のブランチルータから届いたパケットに付与されている第１送信元アドレスと、このパケットを復号化することによって得られる第２送信元アドレスとを取得する取得ステップと、前記取得ステップにおいて得られた前記第２送信元アドレスに基づいて経路情報テーブルを検索し、該当する経路情報が前記トンネル経路であり、かつ

、前記トンネル経路の送信インタフェースがこのパケットを受信したインタフェースと一致するとともに、前記トンネル経路の終端アドレスが前記第１送信元アドレスと一致するか否かを判定する判定ステップと、前記判定ステップにおいて否と判定された場合にはそのパケットを破棄する破棄ステップと、を有する。

このような方法によれば、グループ内の複数のブランチルータで共用する単一のグループ鍵を共用するネットワークシステムにおいて、リダイレクトによるリプレイ攻撃を防止することが可能となる。

【００１２】

また、本発明は、複数のブランチルータを有する１以上のグループと、これら１以上のグループを制御するとともに、各グループを構成する複数の前記ブランチルータに対してＭＰＳＡ情報を配布する配布手段を備えるゲートウェイとを有するネットワークシステムを構成する前記ブランチルータにおいて、前記配布手段によって配布された前記ＭＰＳＡ情報に基づいてトンネル経路に従って相互に暗号化通信を行う通信手段と、他のブランチルータから届いたパケットに付与されている第１送信元アドレスと、このパケットを復号化することによって得られる第２送信元アドレスとを取得する取得手段と、前記取得手段によって得られた前記第２送信元アドレスに基づいて経路情報テーブルを検索し、該当する経路情報が前記トンネル経路であり、かつ、前記トンネル経路の送信インタフェースがこのパケットを受信したインタフェースと一致するとともに、前記トンネル経路の終端アドレスが前記第１送信元アドレスと一致するか否かを判定する判定手段と、前記判定手段によって否と判定された場合にはそのパケットを破棄する破棄手段と、を有する、ことを特徴とする。

このような構成によれば、グループ内の複数のブランチルータで共用する単一のグループ鍵を共用するネットワークシステムにおいて、リダイレクトによるリプレイ攻撃を防止することが可能となる。

【００１３】

また、本発明は、複数のブランチルータを有する１以上のグループと、これら１以上のグループを制御するとともに、各グループを構成する複数の前記ブランチルータに対してＭＰＳＡ情報を配布する配布ステップを備えるゲートウェイとを有するネットワークシステムを構成する前記ブランチルータの制御方法において、前記配布ステップにおいて配布された前記ＭＰＳＡ情報に基づいてトンネル経路に従って相互に暗号化通信を行う通信ステップと、他のブランチルータから届いたパケットに付与されている第１送信元アドレスと、このパケットを復号化することによって得られる第２送信元アドレスとを取得する取得ステップと、前記取得ステップにおいて得られた前記第２送信元アドレスに基づいて経路情報テーブルを検索し、該当する経路情報が前記トンネル経路であり、かつ、前記トンネル経路の送信インタフェースがこのパケットを受信したインタフェースと一致するとともに、前記トンネル経路の終端アドレスが前記第１送信元アドレスと一致するか否かを判定する判定ステップと、前記判定ステップによって否と判定された場合にはそのパケットを破棄する破棄ステップと、を有する、ことを特徴とする。

このような方法によれば、グループ内の複数のブランチルータで共用する単一のグループ鍵を共用するネットワークシステムにおいて、リダイレクトによるリプレイ攻撃を防止することが可能となる。

【発明の効果】

【００１４】

本発明によれば、グループ内の複数のブランチルータで共用する単一のグループ鍵を共用するネットワークシステムにおいて、リダイレクトによるリプレイ攻撃を防止することが可能なネットワークシステム、ブランチルータ、および、これらの制御方法を提供することが可能となる。

【図面の簡単な説明】

【００１５】

【図１】本発明の実施形態に係るネットワークシステムの構成例を示す図である。

【図２】図１に示す実施形態に記載のゲートウェイとブランチルータの詳細な構成例を示す図である。
【図３】図２に示すＭＰＳＡ処理部の詳細な構成例を示す図である。
【図４】ブランチルータの接続例と各部のＩＰアドレスの例を示す図である。
【図５】図４に示すブランチルータが有する経路情報テーブルの一例である。
【図６】ＩＰパケットとＥＳＰパケットのフォーマットの一例を示す図である。
【図７】図６に示すＥＳＰパケットの詳細なフォーマットの一例を示す図である。
【図８】図３に示す送信元アドレス検査部において実行される処理の一例を説明するためのフローチャートである。
【図９】図３に示すＥＳＰ復号部とｕＲＰＦ検査部において実行される処理の一例を説明するためのフローチャートである。
【図１０】本発明の変形実施態様を示す図である。
【図１１】図１０に示す変形実施形態の動作を説明するためのフローチャートである。
【発明を実施するための形態】
【００１６】
次に、本発明の実施形態について説明する。
【００１７】
（Ａ）実施形態の構成の説明
図１は、本発明の実施形態に係るネットワークシステムの構成例を示す図である。この図に示すように、本発明の実施形態に係るネットワークシステムは、ゲートウェイ１０、トランジットネットワーク２０、Ｉ－ＩＰ（Internal-Internet Protocol）ネットワーク３０、ブランチルータ５０，６０、Ｅ－ＩＰ（External-Internet Protocol）クライアントネットワーク７０，８０が存在する。なお、ブランチルータ５０，６０はＭＰＳＡに基づいて暗号化通信を行う。
【００１８】
ここで、ゲートウェイ１０は、ブランチルータ５０，６０との間でＩＫＥｖ２（Internet Key Exchange Protocol Version 2）により確立される鍵交換用の暗号化通信路であるＩＫＥ＿ＳＡ（Security Association）を介してグループ鍵を配布するとともに、ＩＫＥｖ２により確立されるデータ通信用の暗号化通信路であるＣＨＩＬＤ＿ＳＡを介して経路情報をＢＧＰ（Border Gateway Protocol）によって交換する。この経路情報には、あるブランチルータからＭＰＳＡを介して他のブランチルータの配下に存在するＥ－ＩＰクライアントネットワークに到達するために、どのブランチルータを介するべきかを示す情報（終端ＩＰアドレス）が含まれており、例えばＲＦＣ５５６５、ＲＦＣ５５１２およびＲＦＣ５５６６で開示されている技術を用いることにより、このような情報を交換することが可能となる。
【００１９】
トランジットネットワーク２０は、Ｉ－ＩＰネットワーク３０およびＭＰＳＡ４０のトラフィックを中継するネットワークである。
【００２０】
Ｉ－ＩＰネットワーク３０は、トランジットネットワーク２０の上でＣＨＩＬＤ＿ＳＡにより設けられた仮想的なネットワークである。Ｅ－ＩＰクライアントネットワーク７０，８０はクライアントの各拠点に設けられた外部のネットワークである。
【００２１】
図２は、図１に示すゲートウェイ１０およびブランチルータ５０，６０の構成例を示す図である。図２に示すように、ゲートウェイ１０は、パケット送受信部１１、ＳＡ（Security Association）処理部１２、ＩＫＥ（Internet Key Exchange）処理部１３、経路プロトコル処理部１４、ＭＰＳＡ送信部１５、ＭＰＳＡ管理部１６、および、パケット送受信部１７を有している。
【００２２】
ここで、パケット送受信部１１は、ブランチルータ５０，６０との間でパケットの送受

信を行う。ＳＡ処理部１２は、ブランチルータ５０，６０との間でＩＰｓｅｃによる暗号化通信を行う際に、ＩＫＥ処理部１３から通知された認証アルゴリズムや暗号化アルゴリズムに基づくＩＫＥ＿ＳＡもしくはＣＨＩＬＤ＿ＳＡによるＳＡ（Security Association）処理を実行する。この結果、ゲートウェイ１０は、ブランチルータ５０，６０との間で暗号化通信によってグループ鍵を配布することができる。

【００２３】

ＩＫＥ処理部１３は、ＩＰｓｅｃにより暗号化通信を行う前に、ＩＰｓｅｃに必要な暗号化アルゴリズムの決定と暗号鍵の共有を行う処理を実行する。経路プロトコル処理部１４は、経路情報テーブルをブランチルータ５０，６０と交換するための処理を実行する。

【００２４】

ＧＳＡ送信部１５は、ブランチルータ５０，６０に対してグループ鍵を送信する処理を実行する。ＧＳＡ管理部１６は、ブランチルータ５０，６０に送信するグループ鍵を管理する処理部である。パケット送受信部１７は、ブランチルータ５０，６０以外のネットワーク機器と接続され、パケットの送受信を行う。

【００２５】

また、ブランチルータ５０は、パケット送受信部５１、ＳＡ処理部５２、ＩＫＥ処理部５３、経路プロトコル処理部５４、ＧＳＡ受信部５５、ＧＳＡ処理部５６、および、パケット送受信部５７を有している。

【００２６】

ここで、パケット送受信部５１は、ゲートウェイ１０およびブランチルータ６０との間でパケットの送受信を行う。ＳＡ処理部５２は、ゲートウェイ１０との間でＩＰｓｅｃによる暗号化通信を行う際に、ＩＫＥ処理部５３から通知された認証アルゴリズムや暗号化アルゴリズムに基づくＩＫＥ＿ＳＡもしくはＣＨＩＬＤ＿ＳＡによるＳＡ処理を実行する。ＳＡ処理の結果、ブランチルータ５０は、ゲートウェイ１０との間で暗号化通信によってグループ鍵を受け取ることができる。

【００２７】

ＩＫＥ処理部５３は、暗号化通信を行う前に、暗号化通信をおこなうＳＡ処理部５２で必要な暗号化アルゴリズムの決定と暗号鍵の共有を行うための処理を実行する。経路プロトコル処理部５４は、経路情報をゲートウェイ１０と交換するための処理を実行する。

【００２８】

ＭＰＳＡ受信部５５は、ゲートウェイ１０から配布されたグループ鍵を受信する処理を実行する。ＭＰＳＡ処理部５６は、グループ鍵に基づくＳＡ処理を実行する。ＭＰＳＡ処理部５６が扱うパケットはＳＡ処理部５２が扱うＣＨＩＬＤ＿ＳＡと同じＥＳＰ（Encapsulated Security Payload）を用いることが可能で、ＥＳＰのヘッダ部に格納されるＳＰＩ（Security Parameter Index）によって何れのＳＡに属するパケットであるかを識別する。パケット送受信部５７は、Ｅ－ＩＰクライアントネットワーク７０との間でパケットの送受信を行う。

【００２９】

ブランチルータ６０は、ブランチルータ５０と同様の構成とされているので、詳細な説明は省略する。なお、図３では図面を簡略化するためにブランチルータ６０とゲートウェイ１０との接続の図示を省略しているが、ブランチルータ６０はブランチルータ５０と同様にゲートウェイ１０に接続されている。

【００３０】

図３は、図２に示すＭＰＳＡ処理部５６の詳細な構成を示す図である。なお、ＭＰＳＡ処理部６６も同様の構成とされているので、以下ではＭＰＳＡ処理部５６を例に挙げて説明する。

【００３１】

図３に示すように、ＭＰＳＡ処理部５６は、ＭＰＳＡ検索部５６１、ＭＰＳＡテーブル５６２、送信元アドレス検査部５６３、ＥＳＰ復号部５６４、および、ｕＲＰＦ（Unicast Reverse Path Forwarding）検査部５６５を有している。

【００３２】
ここで、ＭＰＳＡ検索部５６１は、ブランチルータ６０との間で通信を行う際に、グループ鍵等に関する合意であるＭＰＳＡをＭＰＳＡテーブル５６２から検索し、該当するＭＰＳＡを取得する。ＭＰＳＡテーブル５６２は、前述したＭＰＳＡを格納するテーブルである。
【００３３】
送信元アドレス検査部５６３は、パケットに付与されたＩＰアドレスの送信元アドレスに基づいて経路情報テーブル５９を参照し、パケットの送信元が正当か否かを判定する。
【００３４】
ＥＳＰ復号部５６４は、ＭＰＳＡテーブル５６２を参照して、暗号化されているパケットを復号化処理する。
【００３５】
ｕＲＰＦ検査部５６５は、経路情報テーブル５９に格納されている経路情報に基づいて、パケットの送信元が正当か否かを判定する。
【００３６】
経路情報テーブル５９は、経路プロトコル処理部５４が取得した経路情報を格納し、この経路情報に基づいて、ルーティング処理が実行される。
【００３７】
（Ｂ）実施形態の動作の説明
つぎに、本発明の実施形態の動作について説明する。以下では、まず、本実施形態の概略の動作について説明した後に、詳細な動作について説明する。
【００３８】
図４は、図１に示すブランチルータ５０，６０とＥ－ＩＰクライアントネットワーク７０，８０の詳細な構成例を示す図である。この図４では、ブランチルータ５０，６０は、トランジットネットワーク２０の上でＭＰＳＡ４０によって相互に接続されている。また、Ｅ－ＩＰクライアントネットワーク７０にはパーソナルコンピュータ７１が接続され、Ｅ－ＩＰクライアントネットワーク８０にはパーソナルコンピュータ８１が接続されている。さらに、パーソナルコンピュータ７１のＩＰアドレスは１７２．１６．０．２であり、パーソナルコンピュータ８１のＩＰアドレスは１７２．１７．０．２であり、Ｅ－ＩＰクライアントネットワーク７０のＩＰアドレスは１７２．１６．０．０／１６であり、Ｅ－ＩＰクライアントネットワーク８０のＩＰアドレスは１７２．１７．０．０／１６である。また、ブランチルータ５０，６０のトランジットネットワーク側のＩＰアドレスはそれぞれ１９２．１６８．１．１，１９２．１６８．１．２であり、これらはＭＰＳＡ４０のそれぞれの終端アドレスである。なお、簡単化のためブランチルータ５０，６０はトランジットネットワークの同じサブネットとして図示しているが、異なるサブネットとすることも可能である。
【００３９】
このような構成において、ゲートウェイ１０とブランチルータ５０のＩＫＥ処理部１３，５３の間で、ＩＫＥ＿ＩＮＩＴ交換によりＩＫＥ＿ＳＡで使用する暗号化アルゴリズム（暗号方式や認証方式）が決定され、鍵交換により暗号鍵が共有される。更にＩＫＥ＿ＳＡを通じ、ＩＰｓｅｃでのＣＨＩＬＤ＿ＳＡを通じた通信で使用される暗号化アルゴリズムが決定され、暗号鍵が共有される。この結果、図１に示すように、ゲートウェイ１０とブランチルータ５０の間に暗号化トンネルとして、ＩＫＥメッセージの交換で使用されるＩＫＥ＿ＳＡとＩＰｓｅｃでの保護対象となるパケットを送受信するＣＨＩＬＤ＿ＳＡが形成される。ＭＰＳＡ送信部１５は、ＭＰＳＡ管理部１６からグループ鍵を受け取り、この暗号化トンネルを介してグループ鍵をブランチルータ５０に送信する。ブランチルータ５０のＭＰＳＡ受信部５５は、ゲートウェイ１０から暗号化アルゴリズムやグループ鍵を受信し、ＭＰＳＡ処理部５６に供給する。更にＣＨＩＬＤ＿ＳＡを介し経路プロトコル処理部１４，５４の間でＲＦＣ５５６５、ＲＦＣ５５１２およびＲＦＣ５５６６に基づくトンネル終端ＩＰアドレス情報をＢＧＰによって交換することで、ブランチルータ５０は、

あるＥ－ＩＰクライアントネットワークへのパケットをＭＰＳＡ４０で接続されるどのブランチルータに転送すべきか（トンネル経路情報）を把握する。

【００４０】

同様の処理は、ゲートウェイ１０とブランチルータ６０の間でも実行され、ブランチルータ６０のＭＰＳＡ受信部６５は、ブランチルータ５０が受信したものと同じグループ鍵をゲートウェイ１０から受信し、ＭＰＳＡ処理部６６に供給する。この結果、ブランチルータ５０とブランチルータ６０が同じグループ鍵を保持することになる。更に、ＣＨＩＬＤ＿ＳＡを開始経路プロトコル処理部１４，６４の間でＲＦＣ５５６５、ＲＦＣ５５１２およびＲＦＣ５５６６に基づくトンネル終端ＩＰアドレスをＢＧＰによって交換することで、ブランチルータ６０は、ブランチルータ５０と同様の経路情報を保持し、あるＥ－ＩＰクライアントネットワークへのパケットをＭＰＳＡ４０で接続されるどのブランチルータに転送すべきかを把握する。

【００４１】

ブランチルータ５０とブランチルータ６０は、このようにして取得したグループ鍵を用いることで、ＩＰｓｅｃでの通信で使用される認証方式や暗号化のパラメータをブランチルータ間で個別に交換することなく、図４に示すように、ブランチルータ５０とブランチルータ６０の間に暗号化トンネルとなるＭＰＳＡ４０が形成され、このＭＰＳＡ４０を介して暗号化通信を行うことが可能となる。なお、図４では簡単化のため、ＭＰＳＡ４０に接続するブランチルータ５０側末端のＩＰアドレスは１９２．１６８．１．１であり、ブランチルータ６０側末端のＩＰアドレスは１９２．１６８．１．２としているが、ＩＰパケットの到達性が確保されるものであれば、任意のアドレスを指定可能である。

【００４２】

図５は、ブランチルータ５０，６０が有している経路情報の一例を示す図である。ここで、図５（Ａ）はブランチルータ５０が有している経路情報であり、図５（Ｂ）はブランチルータ６０が有している経路情報である。図５（Ａ）の上段には、ブランチルータ５０が１７２．１６．０．０／１６のＩＰアドレスを有するＥ－ＩＰクライアントネットワーク７０に直接接続（directly connected）されていることが示されている。また、図５（Ａ）の下段には、ブランチルータ５０が１７２．１７．０．０／１６のＩＰアドレスを有するＥ－ＩＰクライアントネットワーク８０に、インタフェース“Ｔｕｎｎｅｌ０”を通じてＭＰＳＡ４０に接続する終端のＩＰアドレスが１９２．１６８．１．２．であるブランチルータを介して接続されていることが示されている。この図５（Ａ）の下段の情報は、ＢＧＰ等により交換される通常の経路情報に加え、ＲＦＣ５５６５、ＲＦＣ５５１２およびＲＦＣ５５６６によって交換されるトンネル終端ＩＰアドレス情報を再帰的に解決するとともに、ブランチルータ５０、６０自身の設定情報等に基づいて、トンネル終端ＩＰアドレスに向けたインタフェースを、自身のＭＰＳＡに接続するインタフェースである“Ｔｕｎｎｅｌ０”として設定することで得られた経路情報、すなわち、ある宛先にパケットを送信するために次にどのインタフェースを介してどこにパケットを転送するべきかを示す情報である。なお、トンネル経路情報とは、ＭＰＳＡを介してパケット中継する際に利用する経路情報を指し、ＭＰＳＡに接続する自身のトンネルインタフェースを送信インタフェース情報として保持するとともに、そのＭＰＳＡを介して接続する宛先ブランチルータのＭＰＳＡ終端ＩＰアドレスを終端アドレス情報とする経路情報とする。

【００４３】

また、図５（Ｂ）の上段には、ブランチルータ６０が１７２．１７．０．０／１６のＩＰアドレスを有するＥ－ＩＰクライアントネットワーク８０に直接接続（directly connected）されていることが示されている。また、図５（Ｂ）の下段には、ブランチルータ６０が１７２．１６．０．０／１６のＩＰアドレスを有するＥ－ＩＰクライアントネットワーク７０に、インタフェース“Ｔｕｎｎｅｌ０”を通じてＭＰＳＡ４０に接続する終端のＩＰアドレスが１９２．１６８．１．１．であるブランチルータを介して接続されていることが示されている。

【００４４】

以上に示す状況において、例えば、パーソナルコンピュータ７１からパーソナルコンピュータ８１にパケットが送信される場合を想定する。その場合、パーソナルコンピュータ７１は、図６（Ａ）に示すようなＩＰパケット１００をＥ－ＩＰクライアントネットワーク７０に送出する。なお、図６（Ａ）のＩＰヘッダ１０１には、送信先アドレスとしてパーソナルコンピュータ８１のＩＰアドレスである１７２．１７．０．２が付与され、送信元アドレスとしてパーソナルコンピュータ７１のＩＰアドレスである１７２．１６．０．２が付与される。

【００４５】

ブランチルータ５０は、このようなＩＰパケット１００を受信し、ゲートウェイ１０から受信した暗号化アルゴリズムやグループ鍵およびトンネル経路情報に基づき、図６（Ｂ）に示すようなＭＰＳＡ４０に属するＥＳＰパケット２００に変換する。より詳細には、図６（Ａ）に示すＩＰパケット１００に、ＥＳＰヘッダ２０２、ＥＳＰトレーラ２０３を付加する。そして、図６（Ｂ）中にハッチングが施されているＩＰヘッダ１０１、ＴＣＰヘッダ１０２、データ１０３、および、ＥＳＰトレーラ２０３を暗号化する。そして、ＥＳＰヘッダ２０２と暗号化された図６（Ｂ）中のハッチングが施された部分を対象とするＥＳＰ認証データ２０４を付加する。最後に、アウターＩＰヘッダ２０１を付加して、ＥＳＰパケット２００が完成する。なお、ＥＳＰヘッダ２０２は、暗号化トンネルを特定するためのＳＰＩ（Security Parameter Index）およびパケットの順番を示すシーケンス番号および暗号化アルゴリズムに応じた初期化ベクタ値等の情報を有する。また、ＥＳＰトレーラ２０３は、暗号化アルゴリズムに応じて暗号化対象データのバイト数を調整するためのパディングデータおよびその長さを示す情報であるパディング長と、ＥＳＰによって暗号化されるネットワーク層もしくはトランスポート層の情報である次ヘッダとを有している。ＥＳＰ認証データ２０４は、データの完全性をチェックするためのデータであり、ＭＡＣ（Message Authentication Code（メッセージ認証コード））を用いてＥＳＰヘッダ２０２からＥＳＰトレーラ２０３までを対象にして生成したＩＣＶ（Integrity Check Value（インテグリティチェック値））を有している。アウターＩＰヘッダ２０１は、ブランチルータ５０によって新たに付加されるＩＰヘッダである。

【００４６】

図７は、アウターＩＰヘッダ２０１とＩＰヘッダ１０１の構成を示す図である。この図に示すように、アウターＩＰヘッダ２０１はその一部に、宛先アドレス２０１ｄと送信元アドレス２０１ｓを有している。また、ＩＰヘッダ１０１はその一部に、宛先アドレス１０１ｄと送信元アドレス１０１ｓを有している。なお、パーソナルコンピュータ７１からパーソナルコンピュータ８１にパケットが送信される場合、前述のように、ＩＰヘッダ１０１の宛先アドレス１０１ｄはパーソナルコンピュータ８１のＩＰアドレスである１７２．１７．０．２であり、送信元アドレス１０１ｓはパーソナルコンピュータ７１のＩＰアドレスである１７２．１６．０．２である。一方、アウターＩＰヘッダ２０１の宛先アドレス２０１ｄは、ＭＰＳＡ４０の終端のＩＰアドレスである１９２．１６８．１．２であり、送信元アドレス２０１ｓはＭＰＳＡ４０の終端のＩＰアドレスである１９２．１６８．１．１である。

【００４７】

ブランチルータ５０から送信されたＥＳＰパケット２００はＭＰＳＡ４０に属しており、トランジットネットワーク２０を介してブランチルータ６０に届けられる。ブランチルータ６０では、ＥＳＰパケット２００がＭＰＳＡ４０に属していることからこれに接続するインタフェース“Ｔｕｎｎｅｌ０”により受信し、ＭＰＳＡ検索部６６１がＭＰＳＡテーブル６６２からＥＳＰヘッダ２０２のＳＰＩを参照して該当するＭＰＳＡを検索し、ＥＳＰ復号部６６４に供給するとともに、ＥＳＰパケット２００を送信元アドレス検査部６６３に供給する。

【００４８】

送信元アドレス検査部６６３は、アウターＩＰヘッダ２０１の送信元アドレス２０１ｓを取得し、この送信元アドレス２０１ｓを終端アドレスとする経路情報を経路情報テーブ

ル６９から検索する。いまの例では、送信元アドレス２０１ｓはブランチルータ５０のＭＰＳＡ４０に接続する終端のＩＰアドレスである１９２．１６８．１．１であるので、経路情報テーブル６９からは図５（Ｂ）の下段に示す経路情報「１７２．１６．０．０／１６　ｖｉａ　１９２．１６８．１．１．　Ｔｕｎｎｅｌ０」が取得される。つぎに、送信元アドレス検査部６６３は、取得した経路情報を参照し、この経路の転送先インタフェースがＥＳＰパケット２００を受信したインタフェースであるか否かを判定する。いまの例では、受信したインタフェースは“Ｔｕｎｎｅｌ０”であり、取得した経路情報と一致するので、該当すると判定する。その結果、このパケットは、正当なパケットと判定されて、ＥＳＰ復号部６６４に供給される。なお、アウターＩＰヘッダ２０１の送信元アドレス２０１ｓに対応する情報が経路情報テーブル６９に存在しないか、または、インタフェースが一致しない場合には、そのパケットを破棄する。このような処理により、送信元を詐称されたパケットを検出して、復号化処理を行うことなく直ちに破棄することができる。

【００４９】

ＥＳＰ復号部６６４は、送信元アドレス検査部６６３から渡されたパケットを、ＭＰＳＡテーブル６６２から供給されたＭＰＳＡに基づいて復号化し、図６（Ａ）に示す元のＩＰパケット１００を取り出し、アウターＩＰヘッダ２０１の送信元アドレス２０１ｓとともにｕＲＰＦ検査部６６５に渡す。

【００５０】

ｕＲＰＦ検査部６６５は、ＥＳＰ復号部６６４によって復号化されたＩＰパケット１００のＩＰヘッダ１０１から送信元アドレス１０１ｓを取得する。そして、この送信元アドレス１０１ｓをキーとして対応する経路情報を経路情報テーブル６９から検索する。いまの例では、送信元アドレス１０１ｓは、パーソナルコンピュータ７１のＩＰアドレスである１７２．１６．０．２である。このため、経路情報テーブル６９では、図５（Ｂ）に示す下段の経路情報（１７２．１６．０．０／１６を含む情報）が対応しているので、この情報が取得される。つぎに、ｕＲＰＦ検査部６６５は、取得した経路情報が示す転送先インタフェースがＥＳＰパケット２００を受信したインタフェースであり、かつ、そのインタフェースが接続するＭＰＳＡ４０の終端アドレスがＥＳＰパケット２００のアウターＩＰヘッダ２０１の送信元アドレス２０１ｓと一致するか否かを判定する。その結果、これら２つの条件を満たす場合には、このＩＰパケット１００をＥ－ＩＰクライアントネットワーク８０に対して送出し、２つの条件の少なくとも一方を満たさない場合にはこのＩＰパケット１００を破棄する。いまの例では、取得した経路情報が示す転送先インタフェースは“Ｔｕｎｎｅｌ０”でありＥＳＰパケット２００を受信したインタフェースと一致し、また、“Ｔｕｎｎｅｌ０”が接続するＭＰＳＡ４０の終端アドレスである１９２．１６８．１．１は、ＥＳＰパケット２００のアウターＩＰヘッダ２０１の送信元アドレス２０１ｓと同じであるので、双方の条件を満たすと判定され、ＩＰパケット１００がＥ－ＩＰクライアントネットワーク８０に送出される。Ｅ－ＩＰクライアントネットワーク８０に送出されたＩＰパケット１００は、パーソナルコンピュータ８１に受信される。

【００５１】

以上の処理により、パーソナルコンピュータ７１から送信されたＩＰパケット１００がパーソナルコンピュータ８１に受信される。また、ｕＲＰＦ検査部６６５によって、ＩＰヘッダ１０１に含まれている送信元アドレス１０１ｓをキーとして経路情報テーブル６９から経路情報を取得し、取得した経路情報が示す転送先インタフェースがＥＳＰパケット２００を受信したインタフェースであり、かつ、そのインタフェースが接続するＭＰＳＡ４０の終端のアドレスがＥＳＰパケット２００のアウターＩＰヘッダ２０１の送信元アドレス１０１ｓと一致する場合には復号化したＩＰパケット１００をＥ－ＩＰクライアントネットワーク８０に送出し、それ以外の場合にはそのＩＰパケット１００を破棄するようにしたので、正常なパケットが盗聴されて宛先を他のブランチルータ宛に書き換えられて送信された場合であっても、ＩＰパケット１００を破棄することができるので、リダイレクトによるリプレイ攻撃を防ぐことができる。

【００５２】

また、以上の実施形態では、ｕＲＰＦ検査部６６５による検査が実行される前に、送信元アドレス検査部６６３によってＥＳＰパケット２００のアウターＩＰヘッダ２０１の送信元アドレス２０１ｓが経路情報テーブル６９に登録された経路情報のうちＥＳＰパケット２００を受信したインタフェースを転送先インタフェースとした終端アドレスと一致するか否かを判定し、該当しない場合にはそのＥＳＰパケット２００を破棄するようにした。これにより、復号化処理を実行する前に不正なパケットを除外することで、不要な復号化処理を排除して処理の負荷を軽減することができる。

【００５３】

つぎに、図８，９を参照して、ブランチルータ５０，６０において実行される処理の一例について説明する。図８は送信元アドレス検査部６６３において実行される処理の一例を説明するためのフローチャートである。このフローチャートの処理が開始されると、以下のステップが実行される。なお、ブランチルータ５０，６０において実行される処理は同様であるので、以下ではブランチルータ６０を例に挙げて説明する。

【００５４】

ステップＳ１０では、送信元アドレス検査部６６３は、ＥＳＰパケット２００のアウターＩＰヘッダ２０１の送信元アドレス２０１ｓを取得する。例えば、前述のように、パーソナルコンピュータ７１からパーソナルコンピュータ８１にパケットを送る場合、送信元アドレス２０１ｓとして、ＭＰＳＡ４０の終端のＩＰアドレスである１９２．１６８．１．１が取得される。

【００５５】

ステップＳ１１では、送信元アドレス検査部６６３は、経路情報テーブル６９を検索し、ステップＳ１０で取得した送信元アドレス２０１ｓを終端アドレスとする経路情報を検索する。いまの例では、ＩＰアドレスである１９２．１６８．１．１を終端アドレスとする経路情報を検索する。

【００５６】

ステップＳ１２では、送信元アドレス検査部６６３は、ステップＳ１１における検索の結果、送信元アドレス２０１ｓに対応する経路情報がトンネル終端として存在するか否かを判定し、トンネル終端として存在する場合（ステップＳ１２：Ｙｅｓ）には処理を終了し、それ以外の場合（ステップＳ１２：Ｎｏ）にはステップＳ１３に進む。いまの例では、経路情報テーブル６９には、ＩＰアドレスである１９２．１６８．１．１に対応する経路情報（図５（Ｂ）の下段に示す経路情報）が存在し、また、その情報はトンネル経路の終端情報であるのでＹｅｓと判定されて処理を終了する。

【００５７】

ステップＳ１３では、送信元アドレス検査部６６３は、対象となるパケットを破棄する。これにより、不正なパケットを破棄することができる。

【００５８】

つぎに、図９を参照して、ＥＳＰ復号部６６４およびｕＲＰＦ検査部６６５において実行される処理の一例について説明する。図９に示す処理が開始されると、以下のステップが実行される。

【００５９】

ステップＳ３０では、ＥＳＰ復号部６６４は、ＥＳＰパケット２００のアウターＩＰヘッダ２０１の送信元アドレス２０１ｓを取得する。例えば、前述のように、パーソナルコンピュータ７１からパーソナルコンピュータ８１にパケットを送る場合、送信元アドレス２０１ｓとして、ルータ５０がトランジットネットワーク２０に接続するインタフェースのＩＰアドレスである１９２．１６８．１．１が取得される。

【００６０】

ステップＳ３１では、ＥＳＰ復号部６６４は、ＥＳＰパケット２００を復号化する。いまの例では、図６（Ａ）に示すＩＰパケット１００が得られる。

【００６１】

ステップＳ３２では、ｕＲＰＦ検査部６６５は、ＩＰパケット１００のＩＰヘッダ１０

１の送信元アドレス１０１ｓを取得する。いまの例では、ＩＰパケット１００から、パーソナルコンピュータ７１のＩＰアドレスを含む送信元アドレス１０１ｓが取得される。

【００６２】

ステップＳ３３では、ｕＲＰＦ検査部６６５は、ステップＳ３２で取得した送信元アドレス１０１ｓをキーとして、経路情報テーブル６９を検索する。いまの例では、パーソナルコンピュータ７１のＩＰアドレスである１７２．１６．０．２がキーとして経路情報テーブル６９が検索される。

【００６３】

ステップＳ３４では、ｕＲＰＦ検査部６６５は、経路情報テーブル６９に存在する送信元アドレス１０１ｓに対応する経路情報を取得し、取得したトンネル経路情報に含まれる転送先インタフェースと、パケットを受信した受信インタフェースが一致するか否かを判定し、転送先インタフェースと受信インタフェースが一致すると判定した場合（ステップＳ３４：Ｙｅｓ）にはステップＳ３５に進み、それ以外の場合（ステップＳ３４：Ｎｏ）にはステップＳ３６に進む。いまの例では、パーソナルコンピュータ７１のＩＰアドレスである１７２．１６．０．２に対応する経路情報として、図５（Ｂ）の下段の経路情報が存在し、この経路情報はＥＳＰパケット２００を受信したインタフェースを転送先インタフェースとするトンネル経路であるので、Ｙｅｓと判定されてステップＳ３５に進む。

【００６４】

ステップＳ３５では、ｕＲＰＦ検査部６６５は、ステップＳ３３で検索した経路情報の終端アドレスがＥＳＰパケット２００のアウターＩＰヘッダ２０１の送信元アドレス２０１ｓと一致するか否かを判定し、一致する場合（ステップＳ３５：Ｙｅｓ）には処理を終了し、それ以外の場合（ステップＳ３５：Ｎｏ）にはステップＳ３６に進む。いまの例では、ステップＳ３３で検索した経路情報は、図５（Ｂ）の下段の経路情報であり、また、その終端アドレスは１９２．１６８．１．１であり、これはＥＳＰパケット２００のアウターＩＰヘッダ２０１の送信元アドレス２０１ｓと一致するので、Ｙｅｓと判定されて処理を終了する。

【００６５】

ステップＳ３６では、ｕＲＰＦ検査部６６５は、処理対象のパケットを破棄する。

【００６６】

以上の処理によれば、ＩＰヘッダ１０１に含まれている送信元アドレス１０１ｓをキーとして経路情報テーブル６９から経路情報を取得し、取得した経路情報の転送先インタフェースがＥＳＰパケット２００を受信したインタフェースと一致するトンネル経路の情報であり、かつ、そのトンネル経路の終端のアドレスがＥＳＰパケット２００のアウターＩＰヘッダ２０１の送信元アドレス１０１ｓと一致する場合には復号化したＩＰパケット１００をＥ－ＩＰクライアントネットワーク８０に送出する。それ以外の場合にはそのＩＰパケット１００を破棄する。これにより、正常なパケットが盗聴されて宛先を他のブランチルータ宛に書き換えられ、そのブランチルータから転送された場合には、ＩＰパケット１００を破棄するので、リダイレクトによるリプレイ攻撃を防ぐことができる。

【００６７】

（Ｃ）変形実施形態の説明

以上の各実施形態は一例であって、本発明が上述したような場合のみに限定されるものでないことはいうまでもない。例えば、図１に示す実施形態では、ブランチルータが２台の場合を示したが、ブランチルータが３台以上存在する場合であっても、本発明を適用することが可能である。また、図１に示す実施形態では、ブランチルータ５０，６０を有するグループが１つのみの場合を例に挙げて説明したが、２以上のグループが存在し、各グループ内で共通のＭＰＳＡを用いて暗号化通信を行う場合に、本発明を適用することも可能である。

【００６８】

また、図３では、送信元アドレス検査部５６３，６６３を設けて送信元アドレスを検査するようにしたが、この送信元アドレス検査部５６３，６６３については必ずしも設ける

必要はなく、場合によっては除外してもよい。

【００６９】

また、図４では、Ｅ－ＩＰクライアントネットワーク７０，８０が同様なサブネットマスク（マスク長）を有するようにしたが、これらに全く異なるサブネットマスクを割り当てるようにしてもよい。また、ブランチルータ５０、６０は同じサブネットでトランジットネットワーク２０に接続するようにしたが、異なるサブネットとなっていてもよい。

【００７０】

また、図６に示す経路情報テーブルは一例であって、これ以外の形式の経路情報を用いるようにしてもよい。

【００７１】

図１０は、本発明の変形実施態様の一例を示す図である。なお、図１０において、図１と対応する部分には同一の符号を付してその説明を省略する。図１０は図１と比較すると、ブランチルータ１５０およびＥ－ＩＰクライアントネットワーク１７０が追加されている。これら以外の構成は、図１と同様である。図１０では、同じＭＰＳＡ内におけるパケットの転送を禁止することで、なりすましを防ぐことができるとともに、不要なトラフィックの増加を抑制することができる。より詳細には、図１０に示す変形実施形態では、ブランチルータ５０，６０，１５０は、パケットを受信した場合に、そのパケットの送信ＭＰＳＡと受信ＭＰＳＡが同じ場合には、そのパケットを破棄する。例えば、図１０に一点鎖線で示すように、ブランチルータ１５０からブランチルータ５０を経由してブランチルータ６０に転送されるパケットが存在する場合には、ブランチルータ５０が、送信ＭＰＳＡと受信ＭＰＳＡが同じであると判定し、そのパケットを破棄する。これにより、なりすましを防ぐとともに、このようなパケットが転送されてブランチルータ６０において破棄される場合に比較して、不要なパケットの転送を防ぐことで、トラフィックの増加を抑制することができる。

【００７２】

図１１は、図１０に示す変形実施形態のブランチルータ５０，６０，１５０において実行される処理の一例を説明するためのフローチャートである。なお、図１１において、図９と対応する部分には同一の符号を付してその説明を省略する。図１１では、図９と比較すると、ステップＳ３７～Ｓ３９の処理が追加されている。それ以外は、図９と同様である。以下では、ステップＳ３７～Ｓ３９の処理を説明する。

【００７３】

ステップＳ３７では、ｕＲＰＦ検査部６６５は、ＩＰパケット１００のＩＰヘッダ１０１の宛先アドレス１０１ｄを取得する。

【００７４】

ステップＳ３８では、ｕＲＰＦ検査部６６５は、ステップＳ３７で取得した宛先アドレス１０１ｄをキーとして、経路情報テーブル６９を検索する。

【００７５】

ステップＳ３９では、ｕＲＰＦ検査部６６５は、送信ＭＰＳＡと受信ＭＰＳＡが同じか否かを判定し、同じであると判定した場合（ステップＳ３９：Ｙｅｓ）にはステップＳ３６に進んでパケットを廃棄し、それ以外の場合（ステップＳ３９：Ｎｏ）には処理を終了する。

【００７６】

以上の処理によれば、同じＭＰＳＡ内にて転送されるパケットを破棄することで、なりすましを防ぐとともに、不要なトラフィックの増加を抑制することができる。

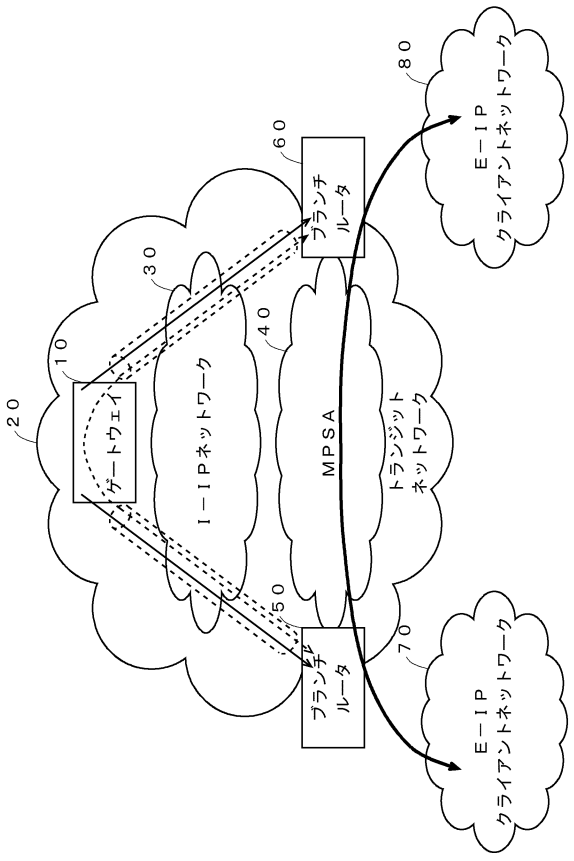
【符号の説明】

【００７７】

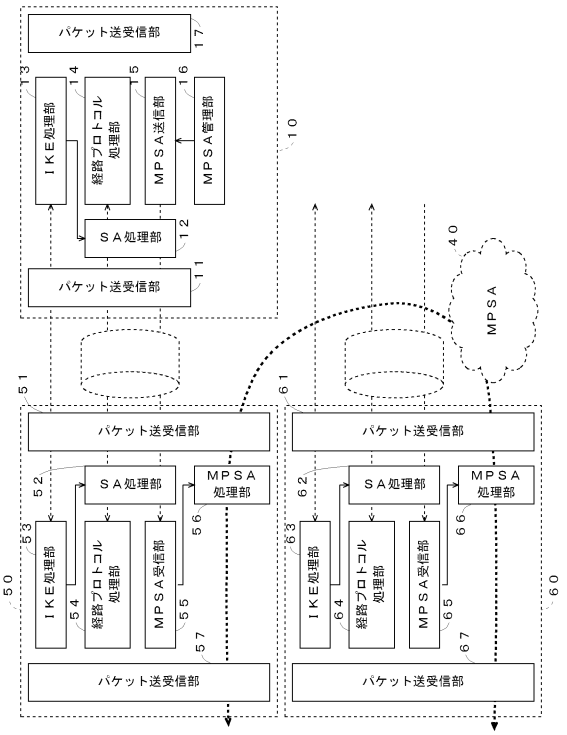
１０　ゲートウェイ
１１　パケット送受信部
１２　ＳＡ処理部
１３　ＩＫＥ処理部

１４　経路プロトコル処理部
１５　ＭＰＳＡ送信部（配布手段）
１６　ＭＰＳＡ管理部
２０　トランジットネットワーク
３０　Ｉ－ＩＰネットワーク
４０　ＭＰＳＡ
５０，６０　ブランチルータ
５１，６１　パケット送受信部（通信手段）
５２，６２　ＳＡ処理部
５３，６３　ＩＫＥ処理部
５４，６４　経路プロトコル処理部
５５，６５　ＭＰＳＡ受信部
５６，６６　ＭＰＳＡ処理部
５７，６７　パケット送受信部
７０，８０　Ｅ－ＩＰクライアントネットワーク
９０　トンネル
５４，６４　経路プロトコル処理部
５６，６６　ＭＰＳＡ処理部
５９，６９　経路情報テーブル
５６１，６６１　ＭＰＳＡ検索部
５６３，６６３　送信元アドレス検査部（取得手段、判定手段、破棄手段）
５６４，６６４　ＥＳＰ復号部（取得手段）
５６５，６６５　ｕＲＰＦ検査部（判定手段、破棄手段）

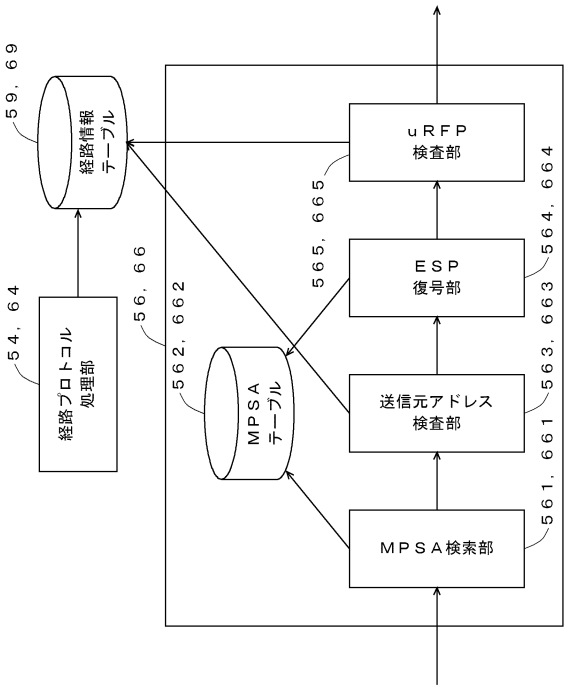
【図１】



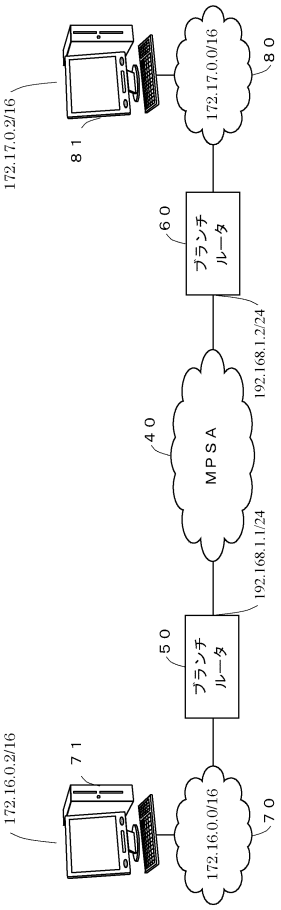
【図２】



【図３】



【図４】



【図５】

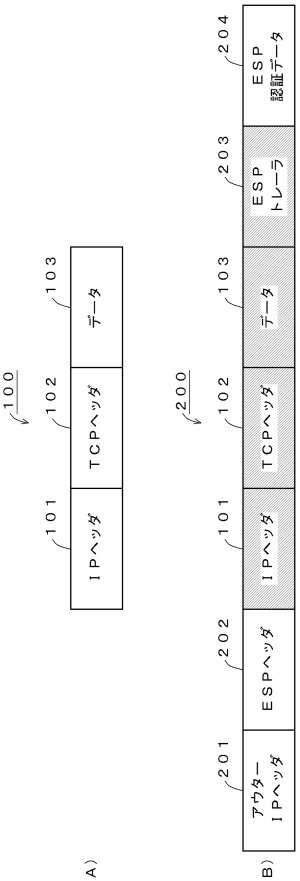
（Ａ）

172.16.0.0/16 is directly connected. E0
172.17.0.0/16 via 192.168.1.2. Tunnel0

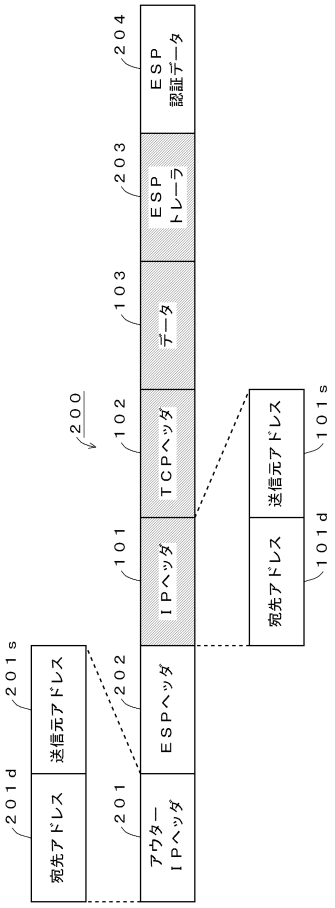
（Ｂ）

172.17.0.0/16 is directly connected. E0
172.16.0.0/16 via 192.168.1.1. Tunnel0

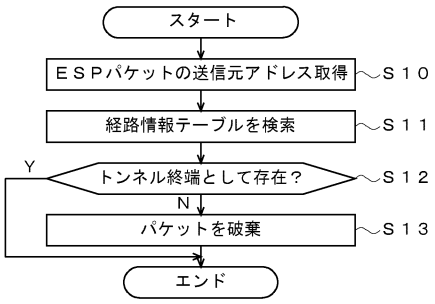
【図６】



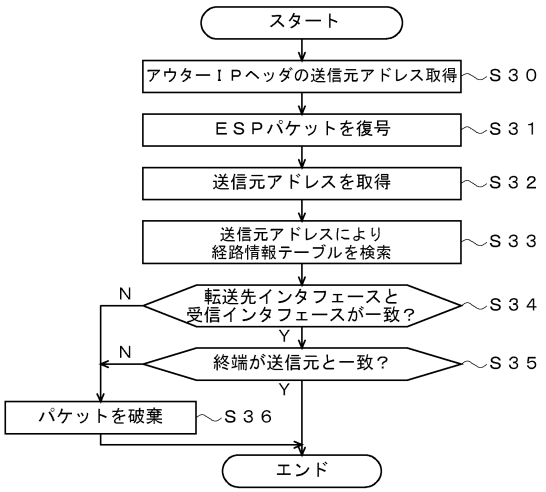
【図７】



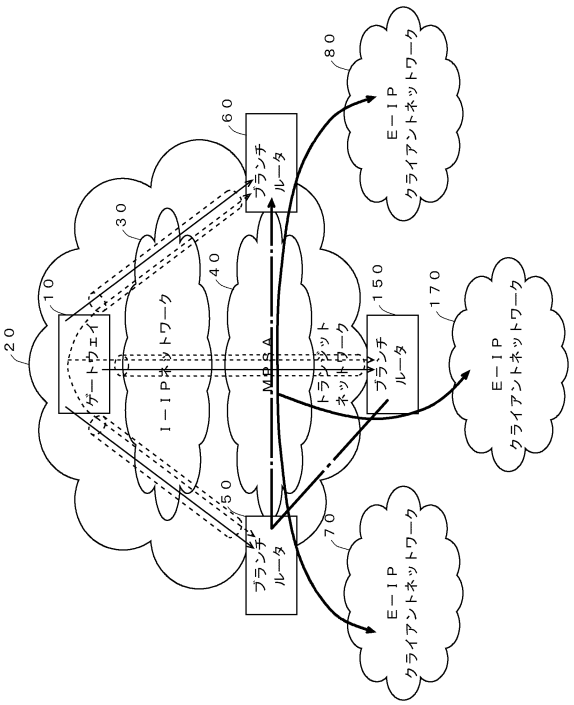
【図８】



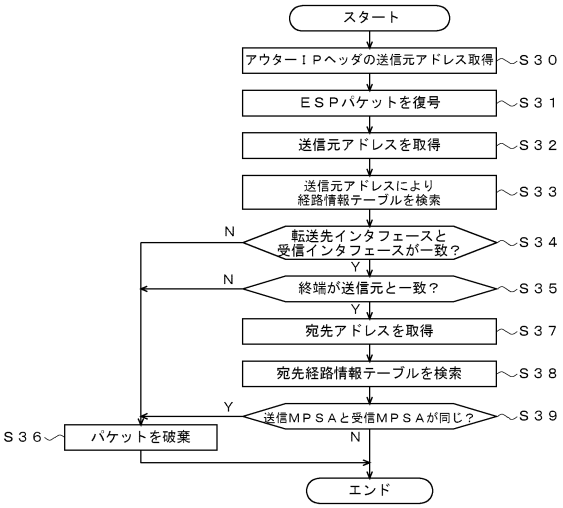
【図９】



【図１０】



【図１１】



フロントページの続き

(72)発明者　山谷　有史
神奈川県平塚市東八幡５丁目１番９号　古河ネットワークソリューション株式会社内
(72)発明者　小林　康宏
神奈川県平塚市東八幡５丁目１番９号　古河ネットワークソリューション株式会社内

審査官　野元　久道

(56)参考文献　特開２０１０－０５０９００（ＪＰ，Ａ）
特開２０１０－４０８８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／６６
Ｈ０４Ｌ　１２／７０