(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4829554号
(P4829554)

(45)発行日　平成23年12月7日(2011.12.7)　(24)登録日　平成23年9月22日(2011.9.22)

(51)Int.Cl.　　F I
G06F 13/00 (2006.01)　　G06F 13/00 351Z
H04L 12/66 (2006.01)　　H04L 12/66 B

請求項の数 16　(全 15 頁)

(21)出願番号　特願2005-200523(P2005-200523)
(22)出願日　平成17年7月8日(2005.7.8)
(65)公開番号　特開2006-40274(P2006-40274A)
(43)公開日　平成18年2月9日(2006.2.9)
審査請求日　平成20年6月16日(2008.6.16)
(31)優先権主張番号　0451496
(32)優先日　平成16年7月9日(2004.7.9)
(33)優先権主張国　フランス(FR)

(73)特許権者　501263810
トムソン　ライセンシング
Ｔｈｏｍｓｏｎ　Ｌｉｃｅｎｓｉｎｇ
フランス国，　９２１３０　イツシー　レ　ムーリノー，　ル　ジヤンヌ　ダルク，　１－５
１－５，　ｒｕｅ　Ｊｅａｎｎｅ　ｄ’Ａｒｃ，　９２１３０　ＩＳＳＹ　ＬＥＳ　ＭＯＵＬＩＮＥＡＵＸ，　Ｆｒａｎｃｅ
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重

最終頁に続く

(54)【発明の名称】装置のグループをプロテクトするファイヤウォール、システムに参加する装置及びシステム内のファイヤウォール・ルールを更新する方法

(57)【特許請求の範囲】
【請求項１】
相互接続可能な装置のグループを保護する分散ファイヤウォールシステムであって、
前記分散ファイヤウォールシステムは、前記グループの各装置で動作するように前記グループの各装置に分散され、前記各装置のどれも前記分散ファイヤウォールシステムで特定の役目を果たさず、
前記グループの各装置は、前記グループの全ての装置について同一である一般グローバルセキュリティポリシーに関する一般情報を管理する手段を有し、
前記グループの各装置は、前記一般グローバルセキュリティポリシーの前記装置の環境への適応に関するローカル情報を管理する手段を有し、
前記ローカル情報は、前記グループに属する装置及び当該装置の接続状態のリストと、ローカルで前記グループにより提供されるサービスのリストとを有し、
前記グループの各装置は、前記一般情報と前記ローカル情報とを使用して、前記一般グローバルセキュリティポリシーのローカルの視野を構成するためのファイヤウォール・ルールを生成する手段を有し、
前記ファイヤウォール・ルールは、前記グループの前記各装置が接続されたネットワーク宛ての通信及び前記グループの前記各装置が接続されたネットワークから生じた通信をフィルタリングするためにフィルタにより使用されるファイヤウォールシステム。
【請求項２】
請求項１に記載のシステムであって、

ローカルセキュリティポリシーを更新し、前記フィルタにより使用されるルールの新しい計算を開始する手段を、前記グループの各装置に有するシステム。

【請求項３】

請求項２に記載のシステムであって、

前記ネットワークで生じる変更に応じて、前記フィルタにより使用されるルールの新しい計算を開始する手段を有するシステム。

【請求項４】

請求項３に記載のシステムであって、

前記フィルタにより使用されるルールの新しい計算を開始するために考慮される変更は、前記グループの装置のネットワークアドレスの変更と、前記グループの装置の追加、除去又は追放と、前記グループの装置によりホストされるサービスの状態の変更とのうち少なくとも１つであるシステム。

【請求項５】

請求項３に記載のシステムであって、

前記フィルタにより使用されるファイヤウォール・ルールの新しい計算を開始するために考慮される変更は、前記グループの装置のネットワークアドレスの変更と、前記グループの装置の追加、除去又は追放と、前記装置でローカルでホストされるサービスの状態の変更とのうち少なくとも１つであるシステム。

【請求項６】

請求項１に記載のシステムであって、

前記グループの装置により提供される少なくとも１つのサービスへの特権アクセスを有する前記グループ外部の装置のリストを決定する手段を、前記グループの各装置に有し、

前記リストは、ローカルセキュリティポリシーと統合されるシステム。

【請求項７】

相互接続可能な装置のグループを保護する分散ファイヤウォールシステムに属する分散ファイヤウォール装置であって、

前記グループの全ての装置について同一である一般グローバルセキュリティポリシーに関する一般情報を管理する手段と、

前記一般グローバルセキュリティポリシーの前記装置の環境への適応に関するローカル情報を管理する手段であり、前記ローカル情報は、前記グループに属する装置及び当該装置の接続状態のリストと、ローカルで前記グループにより提供されるサービスのリストとを有する手段と、

前記一般情報と前記ローカル情報とを使用して、前記一般グローバルセキュリティポリシーのローカルの視野を構成するためのファイヤウォール・ルールを生成する手段であり、前記ファイヤウォール・ルールは、前記グループの前記各装置が接続されたネットワーク宛ての通信及び前記グループの前記各装置が接続されたネットワークから生じた通信をフィルタリングするためにフィルタにより使用される手段と

を有するファイヤウォール装置。

【請求項８】

請求項７に記載の装置であって、

ローカルセキュリティポリシーを更新し、前記フィルタにより使用されるルールの新しい計算を自動的に開始する手段を有する装置。

【請求項９】

請求項８に記載の装置であって、

前記ネットワークで生じる変更に応じてもたらされる前記フィルタにより使用されるルールの新しい計算を開始する手段を有する装置。

【請求項１０】

請求項９に記載の装置であって、

前記フィルタにより使用されるルールの新しい計算を開始するために考慮される変更は、前記グループの装置のネットワークアドレスの変更と、前記グループの装置の追加、除

去又は追放と、前記グループの装置によりホストされるサービスの状態の変更とのうち少なくとも１つである装置。

【請求項１１】

請求項９に記載の装置であって、

前記フィルタにより使用されるファイヤウォール・ルールの新しい計算を開始するために考慮される変更は、前記グループの装置のネットワークアドレスの変更と、前記グループの装置の追加、除去又は追放と、前記装置でローカルでホストされるサービスの状態の変更とのうち少なくとも１つである装置。

【請求項１２】

請求項７に記載の装置であって、

前記グループの装置により提供される少なくとも１つのサービスへの特権アクセスを有する前記グループ外部の装置のリストを決定する手段を有し、

前記リストは、ローカルセキュリティポリシーと統合される装置。

【請求項１３】

分散ファイヤウォールシステムに属する分散ファイヤウォール装置により実施される方法であり、相互接続可能な装置のグループを保護する方法であって、

前記グループの全ての装置について同一である一般グローバルセキュリティポリシーに関する一般情報を管理するステップと、

前記一般グローバルセキュリティポリシーの前記装置の環境への適応に関するローカル情報を管理するステップであり、前記ローカル情報は、前記グループに属する装置及び当該装置の接続状態のリストと、ローカルで前記グループにより提供されるサービスのリストとを有するステップと、

前記一般情報と前記ローカル情報とを使用して、前記一般グローバルセキュリティポリシーのローカルの視野を構成するためのファイヤウォール・ルールを生成するステップであり、前記ファイヤウォール・ルールは、前記グループの前記各装置が接続されたネットワーク宛ての通信及び前記グループの前記各装置が接続されたネットワークから生じた通信をフィルタリングするためにフィルタにより使用されるステップと

を有する方法。

【請求項１４】

請求項１３に記載の方法であって、

前記装置によりホストされるサービスの状態の変更を検出するステップを更に有する方法。

【請求項１５】

請求項１３に記載の方法であって、

前記グループの装置によりホストされるサービスの状態の変更を検出するステップを更に有する方法。

【請求項１６】

請求項１４又は１５に記載の方法であって、

前記ファイヤウォール・ルールの新しい計算の開始は、前記グループの装置の追加、除去又は追放の検出と、前記グループの装置のIPアドレスの変更の検出と、サービスの状態の変更の検出とに関係する方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、相互接続可能な装置のグループの保護に関するものであり、特に、これらの装置とそれらが接続されているネットワークとの間でトラヒックをフィルタリングすることを可能にするファイヤウォール・ルールのポリシーの管理に関するものである。

【背景技術】

【０００２】

ローカルネットワーク、特にドメスティックネットワークは、相互にネットワーク接続

された一式の装置(テレビ、デジタルレコーダ、コンピュータ、携帯情報端末等)から構成されており、ユーザに拡張サービスを提供するように、ユーザにトランスペアレントに自己構成及びインタラクトする。“HPnP™ Device Arcitecture 1.0”に記載されているUPnP、“HAVi Specification Version1.1”に記載されているHAVi、及び“Autoconfiguration for IP networking: Enabling local Communication”、IEEE Internet Computing、2001年5月にE.Guttmanにより記載されているRendezvousは、ドメスティックネットワーク用の標準のいくつかの現在の提案である。ユーザ又はユーザの家族に属している装置は、同一のセキュリティポリシーを共有する。これらの装置は複数のネットワークを介して相互接続可能である。これらのネットワークは、IEEE1394やIEEE Ethernet（登録商標）等のような家庭内の有線ネットワークでもよい。また、IEEE802.11やBluetooth等のような無線ネットワークでもよい。装置はまた、例えばユーザが職場に運んで企業ネットワーク及びインターネットを介して住宅のネットワークと通信する移動体装置のように、インターネットを介して通信してもよい。

【０００３】

このようなグループを広く配備しようとすると、そのグループは保護されなければならない。特に、ユーザの装置に攻撃する動機及び純粋の機会が存在する。ドメスティック装置のグループを保護する最初のステップは、その境界を作ること、すなわちどの装置がグループに属するかを定めることにある。

【０００４】

これらのドメスティックグループを保護する第２のステップは、グループの装置と外部世界との間、又はグループ自体の装置間の通信をフィルタリングするポリシーを定めることである。この種類のフィルタはファイヤウォールと呼ばれ、周知である。複数の種類のファイヤウォールが存在する。

【０００５】

特に、企業ネットワークと外部との間のリンクに配置されたファイヤウォールを企業ネットワークに備えることが知られている。特にこの種類のネットワークでは、ネットワークと外部との間の全ての通信は、１つ以上の明確な接続ポイントを介して通過する。この場合、ファイヤウォールは、セキュリティポリシーを定めてそれを実装する立場の有能な人員により管理される。

【０００６】

一般的にパーソナルファイヤウォールと呼ばれるものを、インターネットに直接連結したパーソナルコンピュータに備えることも知られている。このファイヤウォールは、コンピュータと外部世界との間のネットワークトラフィックをフィルタリングするコンピュータのソフトウェアフィルタである。このフィルタは、ユーザにより定められたポリシーの機能としてもたらされる。このため、ユーザが簡単にこのポリシーを示し、使用されるプロトコル、使用されるサービス又は通信の方向の機能として、パケットフィルタのルールの形式にそれを変換することを可能にするツールが存在する。ユーザのタスクを容易にする目的のこのようなツールにもかかわらず、ユーザは、ファイヤウォールの管理と、コンピュータのセキュリティポリシーに対する変更とを担当する。

【０００７】

外部への複数のアクセスポイントを処理するネットワークのファイヤウォール・ポリシーの管理について、分散ファイヤウォールの概念が作られている。この種類のファイヤウォールでは、セキュリティポリシーは、ポリシーサーバとしての役目をするネットワークのポイントで定められ、複数のポイント(一般的に全てのネットワークアクセスポイント)で適用される。このように、ファイヤウォール・ポリシーの一貫性は、ポリシールール及びその更新を単一ポイントに集中することにより、全体ネットワークで確保される。

【０００８】

現代のドメスティック装置のグループの特徴は、前述の技術のうちの１つに従ったファイヤウォールで保護しようとすると、一定の問題を生じる。本来共有であるRF媒体の使用、インターネットを通じた装置間の通信、向かい合って置かれた装置間でのサービスを見

えるようにすること及び自動交換することは、ドメスティックネットワークの物理的境界及びドメスティックネットワークの装置と外部とのアクセスポイントの位置をあいまいにする複数の要因である。このようなグループにおいて、各装置は、この通信が特定のアクセスポイントを通過する必要なく、ネットワークの外部の装置と通信することができる。

【０００９】

更に、ドメスティックグループの装置は、障害を作り、オフになり、又はグループの残りの通信手段の範囲外にユーザにより持ち去られる傾向がある。従って、一方で、セキュリティポリシーは、住宅から持ち去られる装置と、住宅内に残る装置とに適用されなければならないことが明らかである。従って、グループのセキュリティを確保する特権の役目をする装置のネットワークでの存在を頼りにすることはできない。更に、ポリシーは、グループへの変更、新しい装置の追加又は削除を考慮することが必要である。

【発明の開示】

【発明が解決しようとする課題】

【００１０】

本発明は、ファイヤウォール・ポリシーの分散管理及び完全分散管理を可能にし、各装置のレベルで実装され、一貫性があり、ドメスティックネットワーク内で生じる変化に動的に適応する。ユビキタス・ファイヤウォールと呼ぶ。

【課題を解決するための手段】

【００１１】

本発明は、少なくとも１つの共通のグローバルセキュリティルールのセットを共有する相互接続可能な装置のグループを保護することを可能にするファイヤウォールシステムに関するものであり、グループの各装置は、グローバルセキュリティルールと、グループのメンバのリスト及びその接続状態と、ローカルで提供されるサービスのリストとを少なくとも有するローカルセキュリティポリシーを格納する手段を有し、グループの複数の装置は、接続されているネットワーク宛て及びネットワークからのメッセージのフィルタを有し、システムは中央の手段を有さず、ローカルセキュリティポリシーの機能としてフィルタにより使用されるルールを計算するグループローカル手段を各装置に有する。

【００１２】

本発明の特定の実施例によると、システムは、ローカルセキュリティポリシーを更新し、フィルタにより使用されるルールの新しい計算を開始するグループ手段を各装置に有する。

【００１３】

本発明の特定の実施例によると、システムは、ネットワークで生じる変更に応じて、フィルタにより使用されるルールの新しい計算を開始する手段を有する。

【００１４】

本発明の特定の実施例によると、フィルタにより使用されるルールの新しい計算を開始するために考慮される変更は、グループの装置のネットワークアドレスの変更と、グループの装置の追加、除去又は追放と、グループの装置によりホストされるサービスの状態の変更とのうち少なくとも１つである。

【００１５】

本発明の特定の実施例によると、フィルタにより使用されるファイヤウォール・ルールの新しい計算を開始するために考慮される変更は、グループの装置のネットワークアドレスの変更と、グループの装置の追加、除去又は追放と、装置でローカルでホストされるサービスの状態の変更とのうち少なくとも１つである。

【００１６】

本発明の特定の実施例によると、システムは、グループの装置により提供される少なくとも１つのサービスへの特権アクセスを有するグループ外部の装置のリストを決定するグループ手段を各装置に有し、そのリストは、ローカルセキュリティポリシーと統合される。

【００１７】

本発明はまた、少なくとも１つの共通のグローバルセキュリティルールのセットを共有する相互接続可能な装置のグループに属する手段を有する装置に関するものであり、グローバルセキュリティルールと、グループのメンバのリスト及びその接続状態と、ローカルで提供されるサービスのリストとを少なくとも有するローカルセキュリティポリシーを格納する手段を有し、その装置は、接続されているネットワーク宛て及びネットワークからのメッセージのフィルタを有するファイヤウォールを有し、それにより、それはローカルセキュリティポリシーの機能としてフィルタにより使用されるファイヤウォール・ルールを計算するローカル手段を有し、中央の手段を要求しない。

【００１８】

本発明の特定の実施例によると、装置は、ローカルセキュリティポリシーを更新し、フィルタにより使用されるルールの新しい計算を自動的に開始する手段を有する。

【００１９】

本発明の特定の実施例によると、装置は、ネットワークで生じる変更に応じてもたらされるフィルタにより使用されるルールの新しい計算を開始する手段を有する。

【００２０】

本発明の特定の実施例によると、フィルタにより使用されるルールの新しい計算を開始するために考慮される変更は、グループの装置のネットワークアドレスの変更と、グループの装置の追加、除去又は追放と、グループの装置によりホストされるサービスの状態の変更とのうち少なくとも１つである。

【００２１】

本発明の特定の実施例によると、フィルタにより使用されるファイヤウォール・ルールの新しい計算を開始するために考慮される変更は、グループの装置のネットワークアドレスの変更と、グループの装置の追加、除去又は追放と、装置でローカルでホストされるサービスの状態の変更とのうち少なくとも１つである。

【００２２】

本発明の特定の実施例によると、装置は、グループの装置により提供される少なくとも１つのサービスへの特権アクセスを有するグループ外部の装置のリストを決定する手段を有し、そのリストは、ローカルセキュリティポリシーと統合される。

【００２３】

本発明はまた、方法を実装する装置に接続されたネットワーク宛て及びネットワークからのメッセージのフィルタを有するファイヤウォールにより使用されるルールを更新する方法に関するものであり、装置は、少なくとも１つの共通のグローバルセキュリティルールのセットを共有する相互接続可能な装置のグループの一部を形成し、装置は、グローバルセキュリティルールと、グループのメンバのリスト及びその接続状態と、ローカルで提供されるサービスのリストとを少なくとも有するローカルセキュリティポリシーを格納する手段を有し、そのルールは、ローカルセキュリティポリシーの機能として計算され、

－グループの装置の追加、除去又は追放を検出するステップと、

－グループの装置のネットワークアドレスの変更を検出するステップと、

－ローカルセキュリティポリシーの変更に応じてルールの新しい計算を開始するステップと

のうち少なくとも１つを有する。

【００２４】

本発明の特定の実施例によると、方法は、装置によりホストされるサービスの状態の変更を検出するステップを更に有する。

【００２５】

本発明の特定の実施例によると、方法は、グループの装置によりホストされるサービスの状態の変更を検出するステップを更に有する。

【００２６】

本発明の特定の実施例によると、ファイヤウォール・ルールの新しい計算の開始は、グループの装置の追加、除去又は追放の検出と、グループの装置のIPアドレスの変更の検出

と、サービスの状態の変更の検出とに関係する。

【発明の効果】

【００２７】

本発明は、ファイヤウォール・ポリシーの分散管理を可能にする。

【発明を実施するための最良の形態】

【００２８】

本発明は、以下の説明を読むことで理解され、他の特徴及び利点が明らかになる。

【００２９】

ユビキタス・ファイヤウォール及びそのようなファイヤウォールを使用したセキュリティポリシーの管理の例示的な実施例について説明する。例示的な実施例は、IPプロトコル(“Internet Protocol”)を介して通信するドメスティック装置のグループのフレームワーク内で提供されている。IPプロトコルの仕様は、番号791でIETF(Internet Engineering Task Force)により管理されているRFC(request for comments)にある。しかし、当業者は、例えばIEEE1394等で使用されるプロトコルにかかわらず、本発明が如何なる種類の通信ネットワークにも適用され得ることがわかる。

【００３０】

ドメスティック装置のグループで対処される必要がある制約は以下の通りである。

【００３１】

まず、装置は、いずれかの時点においてもオン又はオフする傾向がある。従って、ネットワークのこれらの装置の出現及び離脱を管理する必要がある。

【００３２】

グループの装置は、グループに属していない装置に物理的に接続されていてもよい。特に無線通信では、物理ネットワークに接続されている装置は、必ずしもグループの一部であるとは限らない。同様に、如何なる装置もグループと外部世界との間のアクセスポイントになる傾向がある。従って、グループを相互接続するネットワークの物理的境界は明確に定まらない。

【００３３】

グループに属する全ての装置がいずれかの時点で相互に通信する立場に必ずしもある必要はない。例えば、家から離れたユーザは、住宅の残りの装置から分離したサブネットワークをその間で構成するデジタルアシスタントと携帯電話通信を行ってもよい。これらの装置は、ドメスティックネットワークの残りから分離して、グループに定められたセキュリティポリシーを適用可能でなければならない。従って、グループは、一時的に相互に通信不可能な任意の数の区分に分離される傾向がある。同様に、装置の環境及び属性が時間に応じて変更してもよい。このように、装置は、例えばネットワークの２つの連続的な接続の間でIPアドレスを変更してもよい。

【００３４】

更に、例えば企業ネットワークで生じたことに対して、ドメスティックグループを管理する有能な管理人の助けを頼ることはできない。特に、一般的にユーザは、ファイヤウォールをカスタマイズする問題を調査する能力又は時間を有さない。しかし、同時に、ユーザはグループに対する唯一の権利者である。従って、ファイヤウォール・ルールにトランスペアレントにセキュリティポリシーを示し、それを変換する簡単な手段を、ユーザに提供する必要がある。

【００３５】

図１は、例示的なドメスティックグループを示している。一方で、ドメスティックグループは、住宅にある空間(参照1.1)の装置と、住宅の外にある空間1.3にある装置とを有する。ここで、これらの２つの空間は相互に通信できないことを仮定する。一方で、住宅1.1の空間は、テレビ1.5と、デジタルビデオレコーダ1.6と、デジタルデコーダ1.7とを連結する優先ネットワークを有し、また、ADSLモデム1.8はインターネット1.4へのアクセスを提供し、例えば802.11ファミリーのプロトコルのうち１つに従って動作する無線端末1.9は、HIFI装置1.10とコンピュータ1.11との接続を可能にする。802.11標準ファミリーは、

ANSI/IEEE文献std802.11-1999(2003年再確認)で標準化された無線ネットワークでの通信の標準を定めている。無線機能を有する近隣のコンピュータ1.14は、ドメスティックグループの一部を形成しないが、無線ネットワーク1.2に物理的に接続することができる。住宅の外のユーザは、例えばBluetoothプロトコルに従った無線接続により、例えばデジタルオーガナイザ1.13及び移動体電話1.12に相互に接続し、グループの区分1.3を作ることができる。この区分は、ユーザが住宅に戻ったときに、グループの残りに再接続されるように求められる。ユビキタス・ファイヤウォール装置(参照1.15)は、各装置に分散しており、グループの装置に現れる灰色の長方形で定められる。

【００３６】

ドメスティック装置のグループのセキュリティを確保するため、セキュリティポリシーを定め、このポリシーを実装可能にすることが必要である。ドメスティックグループのセキュリティポリシーは、従来の企業ネットワークにあり得るものと同様である。それは２つの部分で構成される。

【００３７】

第１の部分は、グループのメンバ構成の問題を生じる。特に、解決されるべき第１の問題は、グループの境界の定義の問題である。ドメスティックグループは、一定のセキュリティポリシーの装置のドメインを構成する。同一のグループの全ての装置は共通のセキュリティポリシーを共有し、高い相互レベルの信用を共有する。一般的に同一のグループの装置は自由に相互に通信できると考えられる。この問題は、例えば、Nicolas Pringent及びJean-Pierre Andreaux による“Gestion securisee de groupes de disposit ifs dans un reseau domestique”(Secure management of groups of devices in a domestic network)、proceedings of the second symposium on securi ty of information and communication technologies(SSTIC2004)の文献に記載されている技術により解決される。この文献では、ユーザが、各装置の暗号証明可能な識別表示を用いてドメスティックグループに属する装置を容易に定めることができる方法について説明している。ユーザは、グループの装置の追加及び除去を管理する立場にある。

【００３８】

グループのセキュリティポリシーの第２の部分は、グループの装置と外部世界との間の通信を管理することを対象とする。従って、これは、グループの装置と、グループに属さないがグループの装置と通信可能な装置との間の通信を含む。このようなものに、インターネットを介してアクセス可能な装置、又はゲストにより住宅に持ち込まれてユーザのドメスティックネットワークに一時的に接続された装置がある。ドメスティックグループの内部の装置はセキュリティポリシーに従うことを前提としているため、グループの一部を形成する装置により開始された通信は、グループを自由に出ることが一般的にわかる。逆に、グループの外部の装置により開始された通信は、監視されなければならず、セキュリティポリシーとの従順性が保証されなければならない。実際に、グループに属する装置により提供されるサービスへのアクセスは、これらのサービスに対する要求がグループの境界で受け取られるために、ユーザにより明示的に許可されなければならない。

【００３９】

より正確には、グループの装置のサービスは、パブリック(すなわち、外部の如何なる装置も同じようにアクセスしてもよい)、制限的(すなわち、外部装置によるこのサービスへのアクセスは条件に左右される)又はプライベート(外部装置によるアクセスは禁じられる)として宣言され得る。従って、グループの外部の装置により開始された通信の従順性をこのポリシーで確認する必要がある。

【００４０】

説明したセキュリティポリシーは一例であり、例示的な実施例のフレームワークを逸脱することなく、このように定められるルールが変更され得ることが明らかである。

【００４１】

このセキュリティポリシーの実装の例示的なモードについて説明する。このため、ユビキタス・ファイヤウォールの概念を定める。前述の制約のため、グループの装置に特定の

役目を行わせることは不可能であり、ドメスティックネットワークのグループの他の装置の存在及びアクセス性を仮定することなく、セキュリティポリシーが全ての装置で確保される必要がある。従って、ユビキタスと呼ばれるファイヤウォールサービスは、グループの各装置のレベルで定められる。

【００４２】

図２はこのサービスのアーキテクチャを示している。それはローカル知識ベース(参照2.1)で構成され、その知識ベースは、ポリシーに関する情報と、装置の現在環境に関する情報とを有する。この情報は、ファイヤウォール・ルールを生成するために、ユビキタス・ファイヤウォールのコア(参照2.5)により使用される。このローカル知識ベース自体は、ローカルポリシーマネージャ(GPL)(参照2.2)を有し、そのタスクは、セキュリティポリシーに関する情報を格納して管理することである。また、ローカル知識ベース自体は、環境適応モジュール(MAE)(参照2.3)を有し、その役目は、装置の環境に関する情報を取得して格納して管理することである。暗号化モジュール(参照2.4)は、ローカル装置と他の装置との間の認証の動作と、場合によってはセキュア通信チャネルを確立するために使用される鍵とをそれ自体に有する。ユビキタス・ファイヤウォール・コア(参照2.5)は、ローカル知識ベースに含まれる情報に基づいて、場合によって暗号化モジュールから得られる鍵を使用することにより、メッセージフィルタ(参照2.6)により使用されるルールを生成することをその内部の一部に有する。メッセージフィルタ(参照2.6)は、このように得られたルールを、ネットワークプロトコルレイヤ(例えばIPレイヤ)から生じたメッセージ及びネットワークプロトコル宛のメッセージに適用する。装置(参照2.8及び2.9)は、トランスペアレントにネットワークプロトコルレイヤにアクセスし、フィルタの適用後のメッセージを受信する。

【００４３】

ローカルポリシーマネージャは、セキュリティポリシーの取得、格納及び管理の役目をする。それは一般グローバルポリシーに関する関連情報を管理し、その一般グローバルポリシーはグループの全ての装置に同一である。このポリシーの例は、以下の２つのルールで作られる。

－ドメスティックグループに属する装置は、セキュアな方法又は他の方法で相互に自由に通信する。

－グループの装置により提供されるサービスへのドメスティックグループの外部の装置によるアクセスは監視される。

【００４４】

この一般ポリシーと、ドメスティックグループに関して有する特別情報(特に、グループの装置のリスト及びその接続状態)と、ローカルで又はグループにより提供されるサービスのリストと、そのパブリック、制限的又はプライベートの状態とを使用することにより、マネージャは、セキュリティポリシーのその独自のローカルの視野を構成することができる。

【００４５】

特に、ローカルポリシーマネージャは、グループの境界に関する第１の種類の情報を有する。それは、主にドメスティックグループに属する装置に関する情報と、それを特定して認証することを可能にする方法に関する情報とを有する。ドメスティックグループの各装置は、証明可能な識別表示を備えており、その証明可能な識別表示により、ネットワークの他の装置で自分を特定して認証することが可能になる。確認が容易であるが、不法使用することが非常に困難であり、暗号化ハードウェアのセキュアな設定を可能にする識別表示のことを、“証明可能な識別表示”と呼ぶ。例えば、鍵の秘密／公開の対のうち公開鍵は証明可能な識別表示として使用されてもよい。その公開鍵で特定されようとする装置は、その秘密鍵を使用してチャレンジ(challenge)に署名することができ、単独でその公開鍵で暗号化されたメッセージを解読することができる。更に、そのそれぞれの証明可能な識別表示を使用することにより、２つの装置はセキュア通信チャネルを作ることができ、例えば鍵に関する合意のプロトコルを使用することにより、特に対称セッション鍵を設

定することが可能になる。このポイント・ツー・ポイントのセッション鍵は、その後の認証に役立ってもよく、２つの装置間の通信(認証及び秘密性)を保護してもよい。

【００４６】

既に引用した“Secure management of groups of devices in a domestic network.”を含み、グループの装置のメンバ構成を信頼できるように確保するための多数の既知の方法が存在する。

【００４７】

ローカルポリシーマネージャは、ドメスティックグループの境界を横断するように許可された通信及びその他のものに関する第２の種類の情報を有する。この種類には、まず、例えばパブリックHTTPサーバのような装置により提供されるパブリックサービスのリストがある。また、制限されたサービスのリストもある。従って、これらのサービスは、特定の条件下でのみアクセス可能である。これらのサービス毎に、マネージャは、このサービスにアクセスするために満たされなければならない条件に関する情報を有する。このような情報の例は、使用される認証方法でのユーザ名及びパスワード、情報の特定の暗号化項目の知識、明示的に許可された装置のリスト、装置が許可されているドメイン、又はその他の条件でもよい。ローカルポリシーマネージャについて複数の情報のソースが存在する。これは、ドメスティックグループのその他の装置のようなセキュリティポリシーのユーザ又は正規のソースでもよい。

【００４８】

ローカルポリシーで生じた特定の変更は、グループの多様な装置間で共有される。これらの変更は複数の形式でもよい。一方で、ユーザはグループの装置を追加、除去又は追放してもよい。追加は、新しい装置がグループの一部を形成すると考えられることをユーザが示した新しい装置に接続されたグループの装置から行われてもよい。装置の除去は、ユーザがグループから取り除こうとする装置で行われてもよく、それに属する他の装置で行われてもよい。追放は、アクセスをもはや有していない装置がグループのメンバとして考えられることを止めなければならないことをユーザがグループに示す手順に関連する。それを実装可能にする機構は、既に引用した“Secure Management of groups of devices in a domestic network”に記載されている。従って、このような変更は、通信する立場になるとすぐに、グループの全ての装置により検討される。

【００４９】

その他の種類のポリシーの変更は、グループの装置のサービスの状態の変更である。ここでは２つの解決策が予想される。第１のものは、装置でホストされているサービスのリストのみがこの装置のローカルポリシーの一部を形成することを示すことにある。これを考慮して、装置で発生したサービスの状態の変更を他の装置で送信する必要はない。この解決策の結果、所定の装置でホストされているサービスの無許可の要求のブロックは、その同じ装置でのみ可能になる。従って、サービスの状態を認識していないネットワークの他の装置は、セキュリティポリシーとの従順性を確認することができずに、要求を中継する。第２の解決策は、グループの全ての装置のサービスの状態に関する情報を送信することにある。この場合、装置のサービスの状態の何らかの変更は、グループの接続中の装置の全てに自動的に送信される。変更時に接続されていない装置での更新は、その次の接続中に生じる。この解決策により、グループの最初の装置に到達するとすぐに、不適合な要求をブロックすることが可能になる。ユーザによるサービスの状態の変更は、サービスをホストする装置でのみ許可され得る。この場合、グループの２つの区分の接続中にポリシーの不一致は存在し得ず、サービスをホストする区分で定められた状態が、他の区分の装置で送信される正確な状態であると常に考えられる。ユーザがグループの何らかの装置からサービスの状態を変更するように許可された場合、所定のサービスについて異なる状態を有するグループの２つの区分が接続されることが生じ得る。状態の最後の変更のスケジュールを考慮することにより、又は２つの状態の間の選択を確認するようにユーザの仲裁を求めることにより、この種類の不一致が解決され得る。

【００５０】

環境適応モジュールは、装置の識別表示と所定の時に有するネットワークアドレス(この例ではIP)との間の関連性の管理をその一部で担う。特に、その証明可能な識別表示によってのみわかる装置にメッセージを送信しようとしているときに、この情報は必須である。このモジュールは、アドレスとグループへのアクセスを有する特権装置の識別表示との間の関連性をも保持する。すなわち、グループの一部を形成していない装置は、グループの特定のサービスへの特権アクセスを有する。このモジュールが装置の識別表示とネットワークでのそのアドレスとの関連性を取得して最新に保つことができる複数の解決策のうち１つは、装置毎に定期的にそのアドレスとその識別表示をネットワークで送信することである。環境適応モジュールがこの種類のメッセージを受信すると、可能な不法使用に対抗するために、この識別表示が正当であることを確認することができる。他の装置のMAEがそれ自体を更新することができるように、定期的な通知メッセージを送信する役目をするのもこのモジュールである。

【００５１】

暗号化データモジュールは、少なくとも２つの主な機能をその一部で有する。一方で、それは装置の証明可能な識別表示の管理の役目をする。他方で、それはまた、セキュア通信チャネルを構築する役目をする。特に、外部の潜在的に悪意のある装置がネットワークに物理的にアクセスすることを回避することができないため、グループの装置間の通信を保護することが有用なことがある。従って、ドメスティックグループの装置を相互にグループ化する仮想プライベートネットワークを作ることができる。ドメスティックネットワーク内の異常な接続属性のため、セキュア通信チャネルの確立は、グループの２つより多い装置の存在を必要としてはならない。グループの有するローカル知識のため、各装置は、他の装置とその通信のポイント・ツー・ポイントのセキュリティを確保する立場にある。性能上の理由で、対称暗号化が好ましいが、非対称暗号化も使用され得ることが明らかである。対称暗号化は、装置へのポイント・ツー・ポイントの鍵の対称な設定を必要とする。使用上の容易性の理由で、これらの対称鍵を定めて装置に入力することをユーザに求めることは不可能である。更に、これはセキュリティのレベルで逆効果である。実際に、ユーザが脆弱な鍵を選択し得るというリスクが存在する。鍵の設定は、例えば、W.DiffieとP.van OorschotとM.Wienerとによる“Authentication and authenticated key exchanges”、Design Codes and Cryptography、2:107-125、1992年の文献に定められているSTS(“Station To Station”)プロトコルを使用することにより行われてもよい。従って、鍵は、使用される鍵の知識を有さないユーザの介入なしに、無条件に設定される。このことにより、良いレベルのセキュリティとシステムの良い人間工学とを得ることが可能になる。ポイント・ツー・ポイント鍵のこのシステムのその他の利点は、装置の変造に対するその抵抗力である。特に、アタッカーが装置の制御を取得すると、鍵がグループの装置の各対の間で厳密にポイント・ツー・ポイントであるという事実のため、他の装置との間の通信は危うくならない。更に、２つの装置がドメスティックグループに存在するとすぐに、システムが動作する。ドメスティックグループの限られたサイズ及び鍵の完全に分散された管理は、装置毎に管理される鍵の数がグループのサイズと共に線形的に増加することを意味し、適度のままになる。

【００５２】

ファイヤウォールのコアは、フィルタにより使用されるファイヤウォール・ルールの生成の役目をする。この生成は、以下のように、ポリシールールに基づいて行われる。

【００５３】

まず、ファイヤウォールは、ユビキタス・ファイヤウォールの動作に必要な通信を許可するルールを確立する。これは、通信可能な装置を通知して検出するためにMAE間で交換されるメッセージと、セキュア通信チャネルが設定されている場合にポイント・ツー・ポイント鍵の認証及び交換を可能にするために暗号化モジュールにより交換されるメッセージとを有する。暗号化モジュール間のこれらのメッセージは、ユビキタス・ファイヤウォールの動作に必須ではないが、ドメスティックグループ内の高レベルのセキュリティを確立するために必要である。ローカル知識ベースの間のメッセージ、及び場合によってはDH

CP要求等のようなネットワークアドレスを取得するために有用なものを許可することも必要である。全てのこれらの通信は、フィルタレベルで保護(暗号化又は認証)が行われずに許可される。

【００５４】

次に、ファイヤウォールのコアは、グループの装置間の通信を可能にするルールを確立する。グループに属するものとして環境適応モジュールにより特定されたアドレスから生じた何らかのメッセージは、既知のソースの証明可能な識別表示、又は暗号化モジュールにより設定された対称鍵若しくは鍵に基づいて、場合によって解読され、その信頼性が確認される。認証が設定されている場合には、認証が正確である場合にメッセージが受け入れられ、その他の場合に拒否される。認証が設定されていない場合、メッセージは受け入れられる。

【００５５】

同様に、グループの装置宛の如何なるメッセージについて、その暗号化及びその認証は、宛先の証明可能な識別表示、又は暗号化モジュールにより設定された対称鍵若しくは鍵に基づいて実行され、送り出される。

【００５６】

ファイヤウォールのコアはまた、特権サービスに関連する通信を規定するルールを定める。ルールは、アクセス条件を確認するための検査を実装しなければならない。例えば、このような証明可能な識別表示を有する装置が所定の特権サービスにアクセスできることをポリシーが示す場合、ここでMAEが使用され、この証明可能な識別表示に対応するIPアドレスを確かめ、それにより、このサービス宛ての要求及びこのアドレスから生じる要求を許可するルールを生成する。共有の秘密を用いて暗号化されたサービスへの要求をフィルタリングするために、IPプロトコルのIPsecのセキュアグループの属性を使用することも可能である。IPsecプロトコルグループの使用は、番号2401でIETF(Internet Engineering Task Force)により管理されているRFC(request for comment)と、それぞれ番号2402と2406と2409でのAHとESPとIKEを構成するプロトコルの一部の記載とにある。他方で、高レベルの認証方法によりアクセスが安全に行われるサービスは、パブリックサービスとして宣言され、この場合、認証はサービスレベルで行われる。この場合、ユーザ名とパスワードとを介してアクセス可能なHTTPサーバへのアクセスが引用されてもよい。この場合、ネットワークプロトコルレイヤのレベルでの検査は不可能である。

【００５７】

ファイヤウォールのコアは、メッセージのソースにかかわらず、パブリックサービスに関する通信を許可するルールを同様に生成する。

【００５８】

最後に、ファイヤウォールのコアは、前述のルールのうちの１つにより明示的に許可されたもの以外の如何なる入力接続を禁止し、如何なる出力接続を許可するルールを生成する。特に、デフォルトでは、全てのサービスはプライベートと考えられる。

【００５９】

これらのルールは、セキュリティポリシーの各変更と共に、又は装置の環境が変更されたときに、再生成される。これらの変更はトポロジーの変更から生じてもよい。すなわち、ネットワークの１つ以上の装置の追加又は除去から生じてもよい。ネットワークの装置の除去(すなわち、グループを出ていない装置の接続の損失)は、ファイヤウォール・ルールの新しい生成を必要としない点に留意すべきである。IPアドレスが変更されていない限り、接続の復帰にしか過ぎない。従って、グループの装置又は特権サービスへのアクセスを許可されているサービスのIPアドレスの変更、グループの装置の除去、追加及び追放のみが、ファイヤウォール・ルールの新しい生成を必要とするイベントである。この変更はまた、グループ内で利用可能なサービスに関するポリシーの変更から生じてもよい。前述のように、この変更は、新しいセットのルールを独自に生成する必要のあるサービスをホストする装置で完全にローカルで管理されてもよく、また、変更がグループ内で送信され、グループの全ての装置での新しい生成を必要としてもよい。この生成が完全に自動化さ

れると、知識のあるセキュリティポリシーに従ったファイヤウォール・ルールのセットが、常に装置に利用可能になる。

【００６０】

ユーザは、グループ内の唯一の権利者である。従って、ユーザのみが、ユーザが有する装置により提供されるサービスの状態(パブリック、プライベート又は制限的)を定めることができる。このため、ユーザは、ユーザが状態を変更しようとしているサービスをホストする装置で、自分を認証する必要がある。装置で自分を認証する方法は、装置に依存し、グループ内で必ずしも均一でない。それは、移動体電話に入力されるコード、又はテレビへのパスワード等を有してもよい。装置に権利者として認証されると、ユーザは、装置により提供されるサービスのリストを提示され、その状態を変更することができる。その状態の変更はまた、制限のあるサービスについて、例えば使用される共有の秘密としてアクセス条件を指定してもよい。

【００６１】

図３は、ファイヤウォール装置を有する装置(参照3.1)の例示的な一般アーキテクチャを示している。このような装置は、ネットワーク(参照3.7)に装置を接続することを目的としたネットワークインタフェース(参照3.6)を有する。それはまた、図２のアーキテクチャに従ってファイヤウォールの実行に必要なプログラムを格納することを目的とした永続的なメモリ(参照3.5)を有する。これらのプログラムは、中央プロセッサ(参照3.2)による実行のため、ランダムアクセスメモリ(参照3.3)にロードされる。全てのこれらの要素は、通信バス(参照3.4)により相互に連結されている。このアーキテクチャはこれらの手段の構成において変更してもよく、ユビキタス・ファイヤウォールを実装することができる装置の例示的なアーキテクチャに過ぎないことが、当業者に明らかである。

【００６２】

このように、ドメスティック装置のグループの各装置で動作するユビキタス・ファイヤウォールについて定義した。このファイヤウォールは、全グループ内の一貫性のある均一のセキュリティポリシーを実装し、通信をフィルタリングすることによりそれを保護する。このファイヤウォールは、各装置に完全に分散され、どの装置もその動作方法において特定の役目を行わない。このポリシーは動的に変更し、グループ内の接続の変更に自動的に適応する。ユーザは、ファイヤウォールの実装の詳細を確認する必要なく、容易にこのポリシーを変更することができる。本発明は、IPベースでないものを含む多様な通信プロトコルに従うネットワークフレームワーク内に実装されてもよく、適用されるセキュリティポリシーのルールを変更すること、又はユビキタス・ファイヤウォールで提示されたアーキテクチャについて機能的な要旨を変更することは、本発明のフレームワークからの逸脱を構成しないことが当業者に明らかである。

【図面の簡単な説明】

【００６３】

【図１】本発明によりプロテクトされるドメスティック装置のグループの全体図

【図２】ユビキタス・ファイヤウォールの装置の例示的な実施例

【図３】ユビキタス・ファイヤウォールを有するドメスティック装置の一般アーキテクチャの例示的な実施例

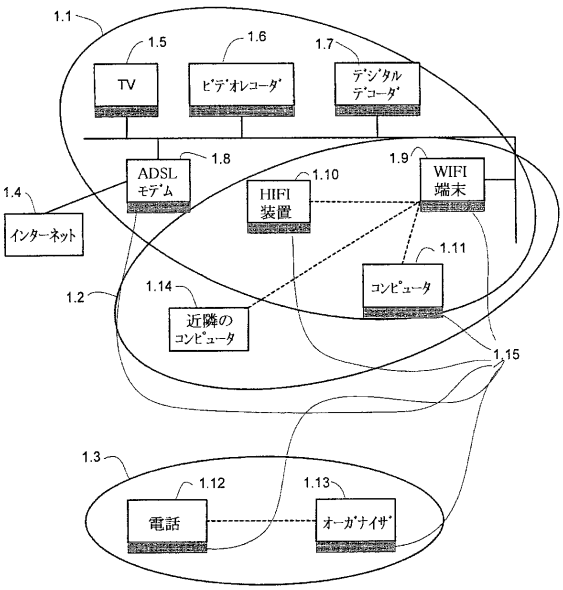
【符号の説明】

【００６４】

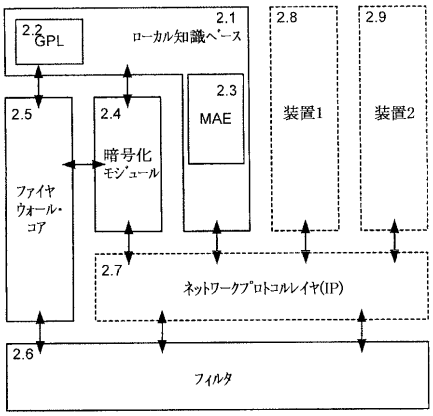
1.1　1.2　1.3　空間
1.4　インターネット
1.5　テレビ
1.6　デジタルビデオレコーダ
1.7　デジタルデコーダ
1.8　ADSLモデム
1.9　WIFI端末
1.10　HIFI装置

1.11　コンピュータ
1.12　移動体電話
1.13　デジタルオーガナイザ
1.14　近隣のコンピュータ
1.15　ユビキタス・ファイヤウォール装置
2.1　ローカル知識ベース
2.2　ローカルポリシーマネージャ(GPL)
2.3　環境適応モジュール(MAE)
2.4　暗号化モジュール
2.5　ユビキタス・ファイヤウォール・コア
2.6　メッセージフィルタ
2.7　ネットワークプロトコルレイヤ(IP)
2.8　装置1
2.9　装置2
3.1　装置
3.2　中央プロセッサ
3.3　ランダムアクセスメモリ
3.4　通信バス
3.5　メモリ
3.6　ネットワークインタフェース
3.7　ネットワーク

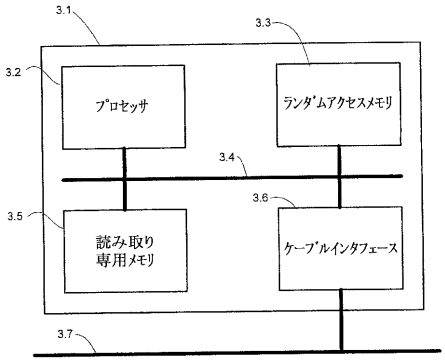
【図１】



【図２】



【図３】



フロントページの続き

(72)発明者　ニコラ　プリジャン
フランス国，３５０００　レンヌ，リュ・アンリ・ル・ギユー　３１，アパルトマン　１０９
(72)発明者　オリヴィエ　イーン
フランス国，３５４１０　ドンルー，リュ・デ・トゥルヌソル　２０
(72)発明者　クリストフ　ビダン
フランス国，３５２３５　トリニェ・フイヤール，リュ・ド・ラ・フォレ　２８
(72)発明者　オリヴィエ　クルテ
フランス国，３５０００　レンヌ，リュ・デュ・ニヴェルネ　１７
(72)発明者　ジャン－ピエール　アンドロー
オランダ国，１０１２　エスペー　アムステルダム，スパイストラート　3エフ2

審査官　田上　隆一

(56)参考文献　特開平０９－２０４３８５（ＪＰ，Ａ）
特開２０００－２５９５２１（ＪＰ，Ａ）
特開２００４－０８６８８０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１３／００