

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5816374号
(P5816374)

(45) 発行日 平成27年11月18日 (2015.11.18)

(24) 登録日 平成27年10月2日 (2015.10.2)

(51) Int. Cl. F I
HO 4 L 12/713 (2013.01) HO 4 L 12/713
HO 4 L 12/803 (2013.01) HO 4 L 12/803

請求項の数 29 (全 16 頁)

(21) 出願番号	特願2014-529854 (P2014-529854)	(73) 特許権者	505418238
(86) (22) 出願日	平成24年9月6日 (2012.9.6)		マカフィー、 インコーポレイテッド
(65) 公表番号	特表2014-529259 (P2014-529259A)		アメリカ合衆国、95054 カリフォル
(43) 公表日	平成26年10月30日 (2014.10.30)		ニア州、サンタ クララ、ミッション カ
(86) 国際出願番号	PCT/US2012/053971		レッジ ブールバード 2821
(87) 国際公開番号	W02013/036646	(74) 代理人	110000877
(87) 国際公開日	平成25年3月14日 (2013.3.14)		龍華国際特許業務法人
審査請求日	平成26年4月16日 (2014.4.16)	(72) 発明者	マイナー、スペンサー
(31) 優先権主張番号	13/227,825		アメリカ合衆国、95054 カリフォル
(32) 優先日	平成23年9月8日 (2011.9.8)		ニア州、サンタ クララ ミッション カ
(33) 優先権主張国	米国 (US)		レッジ ブールバード 2821 マカフ
			イー、インコーポレイテッド内

最終頁に続く

(54) 【発明の名称】 ファイアウォールクラスターにおけるアプリケーション状態共有

(57) 【特許請求の範囲】

【請求項 1】

3つ以上のノードを有するファイアウォールクラスターの第1のノードにおいて、確立されたネットワーク接続のソースポート及び宛先ポートの情報を含む接続状態データを、前記ファイアウォールクラスター内の少なくとも別のノードと共有することと、

前記第1のノードにおいて、前記ネットワーク接続の packets を監視し、前記監視される packets 内のデータパターンを既知のアプリケーションと関連付けられたデータパターンと比較して、いずれのアプリケーションが接続を開始したのかを示すアプリケーション状態データを特定することと、

前記第1のノードにおいて、前記アプリケーション状態データを前記ファイアウォールクラスター内の少なくとも別のノードと共有することと、
を含む、ファイアウォールクラスターを動作させる方法。

【請求項 2】

前記アプリケーション状態データを共有することは、前記アプリケーション状態データを、前記ファイアウォールクラスター内の別のノードにブロードキャストすることを含む、請求項 1 に記載のファイアウォールクラスターを動作させる方法。

【請求項 3】

前記アプリケーション状態データを共有することは、前記アプリケーション状態データをマスターノードに送信することを含む、請求項 1 又は 2 に記載のファイアウォールクラスターを動作させる方法。

10

20

【請求項 4】

前記マスターノードが前記アプリケーション状態データを前記ファイアウォールクラスター内の他のノードにブロードキャストすることを更に含む、請求項 3 に記載のファイアウォールクラスターを動作させる方法。

【請求項 5】

前記第 1 のノードの故障時に、前記別のノードにおいて、前記共有されたアプリケーション状態データを用いて前記ネットワーク接続のデータストリームのフィルタリングを実行することを更に含む、請求項 1 ～ 4 のいずれか 1 項に記載のファイアウォールクラスターを動作させる方法。

【請求項 6】

前記別のノードにおいて、前記共有されたアプリケーション状態データを用いて前記ネットワーク接続のデータストリームのフィルタリングを実行して、前記ファイアウォールクラスターにおける負荷分散を提供することを更に含む、請求項 1 ～ 5 のいずれか 1 項に記載のファイアウォールクラスターを動作させる方法。

【請求項 7】

3 つ以上のノードを有するファイアウォールクラスターの第 1 のノードであって、確立されたネットワーク接続のソースポート及び宛先ポートの情報を含む接続状態データを前記ファイアウォールクラスター内の少なくとも別のノードと共有し、前記ネットワーク接続のパケットを監視し、前記監視されるパケット内のデータパターンを既知のアプリケーションと関連付けられたデータパターンと比較して、いずれのアプリケーションが接続を開始したのかを示すアプリケーション状態データを特定し、前記アプリケーション状態データを前記ファイアウォールクラスター内の少なくとも別のノードと共有するように動作可能な第 1 のノードを備える、ファイアウォールクラスター。

【請求項 8】

前記アプリケーション状態データを共有することは、前記アプリケーション状態データを、前記ファイアウォールクラスター内の別のノードにブロードキャストすることを含む、請求項 7 に記載のファイアウォールクラスター。

【請求項 9】

マスターノードを更に備え、前記アプリケーション状態データを共有することは、前記アプリケーション状態データを前記マスターノードに送信することを含む、請求項 7 又は 8 に記載のファイアウォールクラスター。

【請求項 10】

前記マスターノードは、前記アプリケーション状態データを前記ファイアウォールクラスター内の他のノードにブロードキャストするように更に動作可能である、請求項 9 に記載のファイアウォールクラスター。

【請求項 11】

前記第 1 のノードの故障時に、前記共有されたアプリケーション状態データを用いて前記ネットワーク接続のデータストリームのフィルタリングを実行するように動作可能な第 2 のノードを更に備える、請求項 7 ～ 10 のいずれか 1 項に記載のファイアウォールクラスター。

【請求項 12】

前記共有されたアプリケーション状態データを用いて、前記ネットワーク接続のデータストリームのフィルタリングを実行して、前記ファイアウォールクラスターにおける負荷分散を提供するように動作可能な第 2 のノードを更に備える、請求項 7 ～ 10 のいずれか 1 項に記載のファイアウォールクラスター。

【請求項 13】

コンピュータに、

3 つ以上のノードを有するファイアウォールクラスターの第 1 のノードによって、確立されたネットワーク接続のソースポート及び宛先ポートの情報を含む接続状態データを、前記ファイアウォールクラスター内の少なくとも 1 つのバックアップノードに提供するこ

10

20

30

40

50

とと、

前記第1のノードによって、前記ネットワーク接続のパケットを監視し、前記監視されるパケット内のデータパターンを既知のアプリケーションと関連付けられたデータパターンと比較して、いずれのアプリケーションが接続を開始したのかを示すアプリケーション状態データを特定することと、

前記第1のノードによって、前記アプリケーション状態データを前記ファイアウォールクラスター内の少なくとも1つのバックアップノードに提供することと

を実行させるためのプログラム。

【請求項14】

前記コンピュータに、前記アプリケーション状態データを前記ファイアウォールクラスター内の別の複数のノードにブロードキャストすることをさらに実行させるための、請求項13に記載のプログラム。

【請求項15】

前記コンピュータに、前記アプリケーション状態データを前記ファイアウォールクラスター内のマスターノードに提供することをさらに実行させるための、請求項13又は14に記載のプログラム。

【請求項16】

前記コンピュータに、別のノードにおいて前記ネットワーク接続のデータストリームのフィルタリングを実行し、前記ファイアウォールクラスターにおける負荷分散を提供することをさらに実行させるための、請求項13～15のいずれか一項に記載のプログラム。

【請求項17】

3つ以上のノードを有するファイアウォールクラスターの第1のノードによって、確立されたネットワーク接続のソースポート及び宛先ポートの情報を含む接続状態データを、前記ファイアウォールクラスター内の少なくとも1つのバックアップノードに提供することと、

前記第1のノードによって、前記ネットワーク接続のパケットを監視し、前記監視されるパケット内のデータパターンを既知のアプリケーションと関連付けられたデータパターンと比較して、いずれのアプリケーションが接続を開始したのかを示すアプリケーション状態データを特定することと、

前記第1のノードによって、前記アプリケーション状態データを前記ファイアウォールクラスター内の少なくとも1つのバックアップノードに提供することと

を含む、方法。

【請求項18】

前記アプリケーション状態データを、前記ファイアウォールクラスター内の他の複数のノードにブロードキャストすることを更に含む、請求項17に記載の方法。

【請求項19】

前記アプリケーション状態データを前記ファイアウォールクラスター内のマスターノードに提供することを更に含む、請求項17又は18に記載の方法。

【請求項20】

別のノードにおいて前記ネットワーク接続のデータストリームのフィルタリングを実行し、前記ファイアウォールクラスターにおける負荷分散を提供することを更に含む、請求項17～19のいずれか一項に記載の方法。

【請求項21】

3つ以上のノードを有するファイアウォールクラスターであって、
複数のプロセッサと、
前記複数のプロセッサのうちの1以上と通信可能に接続されたメモリと
を備え、
前記ファイアウォールクラスター内のそれぞれのノードは、前記複数のプロセッサのうちの1以上において動作するべく構成されており、
前記ファイアウォールクラスター内の第1のノードは、

10

20

30

40

50

確立されたネットワーク接続のソースポート及び宛先ポートの情報を含む接続状態データを前記ファイアウォールクラスター内の少なくとも1つのバックアップノードに提供し、前記ネットワーク接続のパケットを監視し、前記監視されるパケット内のデータパターンを既知のアプリケーションと関連付けられたデータパターンと比較して、いずれのアプリケーションが接続を開始したのかを示すアプリケーション状態データを特定し、前記アプリケーション状態データを前記ファイアウォールクラスター内の少なくとも1つのバックアップノードに提供するように動作可能である、ファイアウォールクラスター。

【請求項 2 2】

前記第 1 のノードは、前記 アプリケーション状態データ を、前記ファイアウォールクラスター内の他の複数のノードにブロードキャストするように更に動作可能である、請求項 2 1 に記載のファイアウォールクラスター。

10

【請求項 2 3】

前記第 1 のノードは、前記 アプリケーション状態データ を前記ファイアウォールクラスター内のマスターノードに提供するように更に動作可能である、請求項 2 1 又は 2 2 に記載のファイアウォールクラスター。

【請求項 2 4】

前記マスターノードは、前記 アプリケーション状態データ を前記ファイアウォールクラスター内の他の複数のノードにブロードキャストするように動作可能である、請求項 2 3 に記載のファイアウォールクラスター。

【請求項 2 5】

前記マスターノードは、別のノードにおいて前記 ネットワーク接続のデータストリームのフィルタリングを実行して、前記ファイアウォールクラスターにおける負荷分散を提供するように更に動作可能である、請求項 2 3 又は 2 4 に記載のファイアウォールクラスター。

20

【請求項 2 6】

3 つ以上のノードを有するファイアウォールクラスターのノードであって、

1 以上のプロセッサと、

メモリと

を備え、

前記メモリには、実行された場合に、1 以上のプロセッサに、

前記ファイアウォールクラスターの第 1 のノードによって、確立されたネットワーク接続のソースポート及び宛先ポートの情報を含む接続状態データを格納することと、

30

前記第 1 のノードによって、前記ネットワーク接続のパケットを監視し、前記監視されるパケット内のデータパターンを既知のアプリケーションと関連付けられたデータパターンと比較して、いずれのアプリケーションが接続を開始したのかを示すアプリケーション状態データを特定することと、

前記第 1 のノードの故障に応じて、前記 接続状態データ を前記第 1 のノードから前記ファイアウォールクラスターの第 2 のノードに転送することと、

前記 アプリケーション状態データ を前記第 2 のノードに提供することと

を実行させるための命令が格納されている、ノード。

40

【請求項 2 7】

前記命令は、実行された場合に、1 以上のプロセッサに、前記 アプリケーション状態データ を前記ファイアウォールクラスター内の他の複数のノードにブロードキャストすることを実行させる命令を更に含む、請求項 2 6 に記載のノード。

【請求項 2 8】

前記命令は、実行された場合に、1 以上のプロセッサに、前記 アプリケーション状態データ を前記ファイアウォールクラスター内のマスターノードに提供することを実行させる命令を更に含む、請求項 2 6 又は 2 7 に記載のノード。

【請求項 2 9】

前記命令は、実行された場合に、1 以上のプロセッサに、別のノードにおいて前記 ネッ

50

トワーク接続のデータストリームのフィルタリングを実行して、前記ファイアウォールクラスターにおける負荷分散を提供することを実行させる命令を更に含む、請求項26～28のいずれか一項に記載のノード。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、包括的にはファイアウォール動作に関し、より詳細には、1つの実施形態において、本発明はファイアウォールクラスターにおけるアプリケーション状態共有に関する。

【0002】

〔関連出願の相互参照〕

本出願は、2011年9月8日に出願された米国特許出願第13/227,825号の優先権を主張する。この米国特許出願は、引用することにより本明細書の一部をなす。

【0003】

制限付き著作権放棄

本特許文書の開示の一部は、著作権保護の請求がなされた題材を含む。著作権所有者は、米国特許庁及び商標局のファイル又は記録に見られるように、いかなる者による特許文書又は特許開示のファクシミリ再生に対しても異議はないが、他のいかなる権利についてもそれらの権利の全てを留保する。

【背景技術】

【0004】

コンピューターが有益なツールである所以は主に、コンピューターが他のコンピューターシステムと通信し、コンピューターネットワークを介して情報を取り出すことが可能にある。ネットワークは通常、コンピューター間で情報を転送する能力をコンピューターに与える、配線、光ファイバー、無線、又は他のデータ送信手段によってリンクされた、相互接続されたコンピューター群を含む。インターネットは、おそらく最もよく知られたコンピューターネットワークであり、数百万人の人々が、ウェブページを閲覧するか、電子メールを送信するか、又は他のコンピューター間通信を実行すること等によって、数百万個の他のコンピューターにアクセスすることを可能にする。

【0005】

しかし、インターネットは規模が非常に大きく、インターネットユーザーの関心に非常に多様性があるので、悪意のあるユーザー又は迷惑ユーザー（prankster）が、他のユーザーに危険を課すように他のユーザーのコンピューターと通信することを試みることは珍しくない。例えば、ハッカーは企業のコンピューターにログインして、情報を盗むか、削除するか又は変更するように試みる場合がある。コンピューターウィルス又はトロイの木馬プログラムが他のコンピューターに配信されるか、又は多数のコンピューターユーザーによって知らずにダウンロード若しくは実行される場合がある。さらに、企業等の組織内のコンピューターユーザーは時折、ファイル共有プログラムを実行するか、又は企業のネットワーク内から企業秘密をインターネットに送信する等の認可されていないネットワーク通信を実行しようと試みる場合がある。

【0006】

これらの理由及び他の理由により、多くの企業、団体、及び更にはホームユーザーが、自身のローカルネットワークとインターネットとの間でネットワークファイアウォール又は同様のデバイスを用いる。ファイアウォールは通常、通過するネットワークトラフィックを調査するコンピューター化されたネットワークデバイスであり、1組の規則に基づいて所望のネットワークトラフィックの通過を許可する。

【0007】

ファイアウォールは、TCP/IPパケット又は他のネットワークプロトコルパケット等の通信パケットを観察し、ソースネットワークアドレス及び宛先ネットワークアドレス、いずれのポートが用いられているか、及び接続の状態又は履歴等の特性を検査すること

10

20

30

40

50

によってフィルタリング機能を実行する。ファイアウォールによっては、特定のアプリケーションに対し行き来するパケットも検査するものもあるし、保護されたユーザーと外部のネットワーク化されたコンピューターとの間の選択されたネットワーク要求を処理及び転送することによってプロキシデバイスとして働くものもある。

【0008】

ファイアウォールは通常、ファイアウォール内のネットワークトラフィックを検査すること等によって、様々なポート、ソケット及びプロトコル間の接続を監視することにより、ネットワーク情報のフローを制御する。ソケット、ポート、アプリケーション及び他の情報に基づく規則を用いて、データを選択的にフィルタリングするか又は通過させ、ネットワークアクティビティのログをとる。ファイアウォール規則は通常、ネットワークトラフィックの或る特定のタイプを識別するように構成される。これらのタイプは、禁止されるか、又は或る特定の他の制限が適用されるべきである。他の制限とは、ファイル共有プログラムに用いられることがわかっているポート上のトラフィックをブロックし、一方で従来のFTPポートを介して受信されるいかなるトラフィックもウィルススキャンすること、或る特定のアプリケーション又はユーザーがいくつかのタスクを実行することをブロックし、一方で他のユーザーがそのようなタスクを実行することを可能にすること、及び共通のIPアドレスからの異なるポートに対する反復クエリ等の既知の攻撃パターンに基づいてトラフィックをブロックすること等である。

10

【0009】

しかし、ファイアウォールが、複数のコンピューターシステムにわたって分散されたときにそのような接続を管理する能力は、接続の知識が通常、接続をハンドリングするシステムにしか記憶されないという点で限られている。したがって、クラスターにおける改善されたファイアウォール分散が所望されている。

20

【発明の概要】

【0010】

本発明の様々な例示的な実施形態が、3つ以上のノードを有するファイアウォールクラスターの第1のノードにおいて接続を受信し、第1のノードにおいて、受信した接続のパケットを監視するとともに、監視されているパケットから、接続に関連付けられたアプリケーション状態データを特定し、アプリケーション状態データをファイアウォールクラスター内の少なくとも別のノードと共有するように動作可能な第1のノードを含むファイアウォールクラスターシステムを含む。別のノードは、アプリケーション状態データを用いて、第1のノードが故障した場合等に接続の処理を継続するか、又は負荷分散を提供することができる。

30

【図面の簡単な説明】

【0011】

【図1】本発明のいくつかの実施形態を実施するのに用いることができるような、ファイアウォールを含む例示的なネットワークを示す図である。

【0012】

【図2】本発明のいくつかの実施形態を実施するのに用いることができるような、複数のファイアウォールノードを含むファイアウォールクラスターを含む例示的なネットワークを示す図である。

40

【0013】

【図3】本発明の例示的な実施形態に従う、ファイアウォールクラスター内の共有アプリケーション状態データを用いる方法を示すフローチャートである。

【発明を実施するための形態】

【0014】

本発明の例示的な実施形態の以下の詳細な説明において、図示及び説明のために特定の実施例が参照される。これらの実施例は、当業者が本発明を実施することを可能にするのに十分詳細に説明され、本発明を様々な目的又は実施形態にどのように適用することができるかを示す役割を果たす。本発明の他の実施形態が存在し、これらは本発明の範囲内に

50

あり、本発明の主題又は範囲から逸脱することなく、論理的変更、機械的変更、電気的変更及び他の変更を行うことができる。しかしながら、本明細書において説明される本発明の様々な実施形態の特徴及び制限は、それらが組み込まれる例示的な実施形態に必須なものであり、発明を全体として制限するものではなく、本発明、本発明の要素、動作及び用途へのいかなる言及も、本発明を全体として制限するものではなく、これらの例示的な実施形態を定義する役割のみを果たす。したがって、以下の詳細な説明は本発明の範囲を制限せず、本発明の範囲は添付の特許請求の範囲によってのみ定義される。

【0015】

図1は、101におけるインターネット等の公衆ネットワークと、プライベートネットワーク102と、103に示される、ファイアウォール及び侵入保護機能を提供するよう

10

【0016】

ネットワークデバイス103は、様々な実施形態において、ファイアウォールデバイスであり、侵入保護デバイスであり、又はその双方として機能する。ネットワークデバイス内のファイアウォールデバイス又はモジュールは、ネットワークパケットの調査、及び1組のファイアウォールフィルタリング規則を満たすネットワークパケットのドロップ又は拒否等の様々なネットワークフロー制御機能を提供する。上記で説明したように、ファイアウォールは通常、TCP/IPパケット又は他のネットワークプロトコルパケット等の通信パケットを観察し、ソースネットワークアドレス及び宛先ネットワークアドレス、いずれのポートが用いられているか、及び接続の状態又は履歴等の特性を検査することによってフィルタリング機能を実行する。ファイアウォールによっては、いずれのアプリケーションが接続を確立したかを特定するためにパケットも検査するものもあるし、保護されたユーザーと外部のネットワーク化されたコンピューターとの間の選択されたネットワーク要求を処理及び転送することによってプロキシデバイスとして働くものもある。ファイアウォールは多くの場合に、望ましくないトラフィックの「シグネチャ」又は他の特性を用いて、有害であるとみなされるか又は他の形で望ましくないトラフィックを検出しブロックする。

20

30

【0017】

ファイアウォールは通常、1組の規則を用いてトラフィックをフィルタリングし、ネットワークデータの任意の特定の要素に関して行われることが、その特定のデータにどのように規則の組が適用されるかに依拠するようにする。例えば、ポート6346への全てのトラフィックをブロックする規則は、保護されたネットワーク内のサーバー上のそのポートに向けられた着信トラフィックをブロックするが、同じサーバーの異なるポート番号に向かう他のデータはブロックしない。同様に、Shareaza等のファイル共有プログラムから発信されたトラフィックをブロックする規則は、トラフィックにおけるパターンを用いて、ポート6346上のShareazaトラフィックをブロックするが、ポート6346上の他のトラフィックは許可する。

40

【0018】

しかし、大型のシステム又は複雑なシステム等の、ファイアウォールが複数のコンピューター又はノードにわたって分散されたシステムとして実施される環境では、複数のノードが接続を共有する能力は、接続に関するソケット情報、アプリケーション情報等のような、接続に関する管理ノードの情報に限定される。したがって、本発明のいくつかの実施形態は、クラスターファイアウォール内の他のシステムと、アプリケーションタイプ又は他のそのような接続データ等の状態情報を共有し、ファイアウォールクラスター内の複数のノードが同じ接続を処理することを可能にするメカニズムを提供する。これによって、システム間で接続の担当を移すことによって負荷分散を行い、クラスター内のノードの故障を、そのノードの接続を別のマシンに移すことによって管理し、他のそのような機能を

50

実行する能力がクラスターに与えられる。

【0019】

1つのそのような例において、ファイアウォール又は侵入保護システムは、ファイアウォールを通して流れる処理トラフィックを共有するノードのクラスター又は接続された群として実装される。図2は、本発明のいくつかの実施形態を実施するのに用いることができるような、分散ファイアウォールを有するネットワークを示している。ここで、インターネット201等のネットワークは、ファイアウォール203によって内部ネットワーク202に結合される。ファイアウォール203は、負荷分散及び他のファイアウォール管理機能等の機能を実行することができる着信トラフィックモジュール204及び発信トラフィックモジュール205を含む。ファイアウォール又は侵入保護規則はファイアウォールノード206において適用され、これらのファイアウォールノードは図示されるようにネットワーク接続によって互いに接続される。

10

【0020】

ここで、示される5つのノードはそれぞれ、インターネット201と内部ネットワーク202との間を流れるトラフィックを選択的に許可又はブロックする規則をトラフィックに適用するように動作可能な、ファイアウォール又は関連するソフトウェアのインスタンスを実行する別個のコンピューターシステムを備える。代替の実施形態では、ノード1、ノード2及びノード3等のいくつかのノードがファイアウォールアプリケーションを実行する一方、4及び5等の他のノードは侵入保護システム（IPS）アプリケーションを実行する。ノード204及び205は、ファイアウォールノード206にルーティングされるトラフィックの負荷分散等の機能の実行を担当し、これらのノードが、単一ノードの場合よりも高いスループット能力を提供するように効率的にともに機能することができることを確保する。

20

【0021】

いくつかのファイアウォール実施形態は、ポート、IP及び他のそのような規則をデータストリームに単に適用することを超える、複雑な接続識別機能を実行する。例えば、いくつかのファイアウォールの例は、新たな接続の最初のいくつかのパケットを監視し、アプリケーション通信プロファイル情報に基づいて、接続を開始したアプリケーションを識別するように動作可能なアプリケーション識別モジュールを含む。アプリケーションが特定されると、アプリケーション固有の（application-specific）規則を接続に適用し、ファイアウォールを通して流れるデータを制御する向上した機能を提供することができる。

30

【0022】

206におけるファイアウォールノードが故障した場合、単純に別のノードが接続をピックアップし、ポート、IPアドレス及び他のそのような特性に基づいて、同じ従来のファイアウォール規則を適用することができる。しかし、図2の206における5つの異なるファイアウォールノードは、ポート及びIPアドレス等の識別可能な特性に基づいて接続に同じ規則を適用することができるものの、アプリケーションに基づく規則を接続に適用するように既に確立されたリンクの最初のいくつかのパケットを再検査することができない。

【0023】

したがって、本発明のいくつかの実施形態は、ファイアウォールクラスター内のノードにわたるアプリケーション状態共有のメカニズムを提供し、負荷分散、又は故障したクラスターノードからの復元等のために、ファイアウォールが、アプリケーションに基づく規則が課された接続を別のノードに移すことを可能にする。1つの実施形態において、この状態共有は、図2に示すもの等のように、ファイアウォールクラスター内のノードを互いにリンクするネットワーク接続を介して処理される。アプリケーション情報を含む接続のセッション情報は複数のノードにわたって共有されるので、識別されたアプリケーションとの確立された接続を受信したノードは、ファイアウォール構成によって特定されるようにトラフィックを許可又は拒否するアプリケーション固有の規則を適用することができる。

40

50

【0024】

いくつかの実施形態における状態共有は、状態情報をファイアウォールクラスター内の全ての他のノードにブロードキャストすることを含み、他のノードがそれぞれ、他のノードにおける接続のアプリケーション状態の知識を有するようにする。代替の実施形態では、マスターノードがアプリケーション状態データを受信し、このデータを記憶し、クラスター内の少なくとも2つのノードが、アプリケーション状態データが識別された接続のアプリケーション状態データを有するようにする。したがって、マスターノードは自身のアプリケーション状態データをバックアップマスターノード又は他の指定されたノードと共有し、マスターノードの故障により結果としてアプリケーション状態データが失われないようにすることができる。更に他の例では、マスターノードはアプリケーション状態情報を受信し、次にこの情報を他のノードにブロードキャストする。

10

【0025】

図3は、本発明の例示的な実施形態に従って、ファイアウォール内の複数のノードにわたるアプリケーション状態共有を用いて、ノード故障(failed node)から復元する例を示している。301において、ローカルネットワーク202内のコンピューターとインターネット201との間でリンクが開始される。ノード間のリンクは、ノード1によって処理される。302において、ノード1は、ネットワーク接続が確立されるとすぐに、ソースポート及び宛先ポート並びにIPアドレス等の状態情報を共有する。データのいくつかのパケットがローカルコンピューターとインターネットサーバーとの間で交換された後、303において、ファイアウォールはパケット内のデータパターンを、既知のアプリケーションと関連付けられたデータパターンと比較し、多くの場合に、いずれのアプリケーションが接続を開始したのかを特定することができる。次に、304において、ファイアウォールノード1は、接続に関するこのアプリケーション状態データを他のノードと共有し、305において、このアプリケーション状態データを用いて、アプリケーション固有の規則をファイアウォールに適用する。

20

【0026】

306において、ノード1が故障し、307において、接続がノード2にリダイレクトされる。ノード2は、ノード1から接続に関するアプリケーション状態データを以前に受信しているので、308において、ノード2は、アプリケーション固有の規則を接続に適用することを含む、データストリームのフィルタリングを再開することができる。

30

【0027】

この例は、ノードが故障した後に、ノードが接続のフィルタリングをどのように再開することができるかを示しているが、負荷分散、又は様々なタスクへのノードの再割当て等の用途で、分散ファイアウォールクラスター内で接続をノード間で移すのに、同様の方法を用いることができる。

【0028】

1つのそのような例では、ファイアウォールノード1が故障するのではなく、2つの侵入保護システムノード(図示せず)の一方である侵入保護システムノードが故障する。システムは、ファイアウォールサービスを提供するノード数と、侵入保護を提供するノード数との間で或る特定のバランスを維持することを所望し、この例では、侵入保護システムは、その2つのノードのうちの一方が故障したとき、機能の半分を失っている。したがって、システムは、故障した侵入保護ノードに置き換わるようにファイアウォールノード1を再割当てし、その結果、図2に示すように、以前にファイアウォールノード1によって処理されていた接続は、ファイアウォールノード2～5にわたって再分散される。

40

【0029】

これらの例は、ファイアウォールクラスター内でアプリケーション状態データを共有することによって、ファイアウォールクラスター内の負荷分散、フェイルオーバー及び他の機能をどのように容易にし、ファイアウォールクラスターにおけるネットワークトラフィックのアプリケーションに基づくフィルタリングをより扱いやすく信頼性の高いものにすることができるかを示している。

50

【0030】

本明細書において、特定の実施形態が示され、説明されたが、当業者であれば、同じ目的を果たすように計算された任意の構成を、示された特定の実施形態に置き換えることができることを理解するであろう。本出願は、本明細書に説明した本発明の例示的な実施形態の任意の適応又は変形を包含するように意図される。本発明は特許請求の範囲及びその等価物の全範囲によってのみ限定されることが意図される。

【0031】

1つの例示的な実施形態では、ファイアウォールクラスターを動作させる方法が、3つ以上のノードを有するファイアウォールクラスターの第1のノードにおいて接続を受信することと、第1のノードにおいて、受信した接続のパケットを監視するとともに、これらの監視されるパケットから、接続に関連付けられたアプリケーション状態データを特定することと、アプリケーション状態データをファイアウォールクラスター内の少なくとも別のノードと共有することとからなるプロセスを含む。この例は、接続を受信した後であるが、アプリケーション状態データを共有する前に、受信した接続に関する接続情報をファイアウォールクラスター内の少なくとも別のノードと更に共有することができる。オプションで、ファイアウォールクラスターは、接続に関連付けられたアプリケーションの識別情報を含むアプリケーション状態データを維持することができる。アプリケーション状態データを共有することは、アプリケーション状態データを、ファイアウォールクラスター内の他のノードにブロードキャストすること、又はアプリケーション状態データをマスターノードに送信することを含むことができる。マスターノードは、アプリケーション状態データをファイアウォールクラスター内の他のノードにブロードキャストするように構成することもできる。ファイアウォールクラスターはまた、接続に関連付けられた共有されたアプリケーション状態データを用いて、第1のノードの故障時に別のノードにおいて接続をフィルタリングすることもできるし、接続に関連付けられた共有されたアプリケーション状態データを用いて、別のノードにおいて接続をフィルタリングし、ファイアウォールクラスターにおける負荷分散を提供することもできる。

【0032】

別の例では、ファイアウォールクラスターが第1のノードを備えることができ、この第1のノードは、3つ以上のノードを有するファイアウォールクラスターにおいて接続を受信し、この第1のノードにおいて、受信した接続のパケットを監視するとともに、これらの監視されるパケットから、接続に関連付けられたアプリケーション状態データを特定し、アプリケーション状態データをファイアウォールクラスター内の少なくとも別のノードと共有するように動作可能である。第1のノードは、接続を受信した後であるが、アプリケーション状態データを共有する前に、受信した接続に関する接続情報をファイアウォールクラスター内の少なくとも別のノードと共有するように更に動作可能とすることもできる。この例は当然ながら、上記の例において説明したいくつかの要素又は全ての要素を含むことができる。

[項目1]

3つ以上のノードを有するファイアウォールクラスターの第1のノードにおいて接続を受信することと、

前記第1のノードにおいて、前記受信した接続のパケットを監視し、前記監視されるパケットから、前記接続に関連付けられたアプリケーション状態データを特定することと、

アプリケーション状態データを前記ファイアウォールクラスター内の少なくとも別のノードと共有することと、

を含む、ファイアウォールクラスターを動作させる方法。

[項目2]

前記接続を受信した後であるが、アプリケーション状態データを共有する前に、前記受信した接続に関する接続情報を前記ファイアウォールクラスター内の少なくとも別のノードと共有することを更に含む、項目1に記載のファイアウォールクラスターを動作させる方法。

[項目 3]

アプリケーション状態データは、前記接続に関連付けられたアプリケーションの識別情報を含む、項目 1 又は 2 に記載のファイアウォールクラスターを動作させる方法。

[項目 4]

アプリケーション状態データを共有することは、前記アプリケーション状態データを、前記ファイアウォールクラスター内の他のノードにブロードキャストすることを含む、項目 1～3 のいずれか 1 項に記載のファイアウォールクラスターを動作させる方法。

[項目 5]

アプリケーション状態データを共有することは、前記アプリケーション状態データをマスターノードに送信することを含む、項目 1～4 のいずれか 1 項に記載のファイアウォールクラスターを動作させる方法。

10

[項目 6]

前記マスターノードが前記アプリケーション状態データを前記ファイアウォールクラスター内の他のノードにブロードキャストすることを更に含む、項目 5 に記載のファイアウォールクラスターを動作させる方法。

[項目 7]

前記接続に関連付けられた前記共有されたアプリケーション状態データを用いて、前記第 1 のノードの故障時に別のノードにおいて前記接続をフィルタリングすることを更に含む、項目 1～6 のいずれか 1 項に記載のファイアウォールクラスターを動作させる方法。

[項目 8]

前記接続に関連付けられた前記共有されたアプリケーション状態データを用いて、別のノードにおいて前記接続をフィルタリングし、前記ファイアウォールクラスターにおける負荷分散を提供することを更に含む、項目 1～7 のいずれか 1 項に記載のファイアウォールクラスターを動作させる方法。

20

[項目 9]

第 1 のノードであって、3 つ以上のノードを有するファイアウォールクラスターにおいて接続を受信し、前記第 1 のノードにおいて、前記受信した接続のパケットを監視するとともに、前記監視されるパケットから、前記接続に関連付けられたアプリケーション状態データを特定し、アプリケーション状態データを前記ファイアウォールクラスター内の少なくとも別のノードと共有するように動作可能な第 1 のノードを備える、ファイアウォールクラスター。

30

[項目 10]

前記第 1 のノードは、前記接続を受信した後であるが、アプリケーション状態データを共有する前に、前記受信した接続に関する接続情報を前記ファイアウォールクラスター内の少なくとも別のノードと共有するように更に動作可能である、項目 9 に記載のファイアウォールクラスター。

[項目 11]

アプリケーション状態データは、前記接続に関連付けられたアプリケーションの識別情報を含む、項目 9 又は 10 に記載のファイアウォールクラスター。

[項目 12]

アプリケーション状態データを共有することは、前記アプリケーション状態データを、前記ファイアウォールクラスター内の他のノードにブロードキャストすることを含む、項目 9～11 のいずれか 1 項に記載のファイアウォールクラスター。

40

[項目 13]

マスターノードを更に備え、前記アプリケーション状態データを共有することは、前記アプリケーション状態データを前記マスターノードに送信することを含む、項目 9～12 のいずれか 1 項に記載のファイアウォールクラスター。

[項目 14]

前記マスターノードは、前記アプリケーション状態データを前記ファイアウォールクラスター内の他のノードにブロードキャストするように更に動作可能である、項目 13 に記

50

載のファイアウォールクラスター。

[項目 1 5]

前記接続に関連付けられた前記共有されたアプリケーション状態データを用いて、前記第 1 のノードの故障時に別のノードにおいて前記接続をフィルタリングするように動作可能な第 2 のノードを更に備える、項目 9 ～ 1 4 のいずれか 1 項に記載のファイアウォールクラスター。

[項目 1 6]

前記接続に関連付けられた前記共有されたアプリケーション状態データを用いて別のノードにおいて前記接続をフィルタリングし、前記ファイアウォールクラスターにおける負荷分散を提供するように動作可能な第 2 のノードを更に備える、項目 9 ～ 1 5 のいずれか 1 項に記載のファイアウォールクラスター。

[項目 1 7]

ファイアウォールクラスターを動作させる方法であって、
3 つ以上のノードを有するファイアウォールクラスターの第 1 のノードにおいて接続を受信することと、

前記受信した接続に関する接続情報を前記ファイアウォールクラスター内の少なくとも別のノードと共有することと、

前記第 1 のノードにおいて、前記受信した接続のパケットを監視するとともに、前記監視されるパケットから、前記接続に関連付けられたアプリケーションを特定することと、

前記接続に関連付けられたアプリケーションを示すデータを、前記ファイアウォールクラスター内の 2 つ以上の他のノードと共有することと、
を含む、ファイアウォールクラスターを動作させる方法。

[項目 1 8]

前記接続に関連付けられた前記アプリケーションを示す前記データを用いて、前記第 1 のノードの故障時に別のノードにおいて前記接続をフィルタリングすることを更に含む、項目 1 7 に記載のファイアウォールクラスターを動作させる方法。

[項目 1 9]

前記接続に関連付けられた前記アプリケーションを示す前記データを用いて、別のノードにおいて前記接続をフィルタリングし、前記ファイアウォールクラスターにおける負荷分散を提供することを更に含む、項目 1 7 又は 1 8 に記載のファイアウォールクラスターを動作させる方法。

[項目 2 0]

コンピュータに、
3 つ以上のノードを有するファイアウォールクラスターの第 1 のノードによって、パケットに関連付けられた接続情報を処理することと、

接続を確立することと、
前記接続に関連付けられた状態データを前記ファイアウォールクラスター内の少なくとも 1 つのバックアップノードに提供することと、

前記第 1 のノードの故障に応じて、前記接続を前記クラスターの第 2 のノードに転送することと、

前記状態データを前記バックアップノードから前記第 2 のノードに提供することと
を実行させるためのプログラム。

[項目 2 1]

前記コンピュータに、前記状態データを前記ファイアウォールクラスター内の他の複数のノードにブロードキャストすることをさらに実行させるための、項目 2 0 に記載のプログラム。

[項目 2 2]

前記コンピュータに、前記状態データを前記ファイアウォールクラスター内のマスターノードに提供することをさらに実行させるための、項目 2 0 又は 2 1 に記載のプログラム

。

10

20

30

40

50

[項目 2 3]

前記コンピュータに、別のノードにおいて前記接続をフィルタリングし、前記ファイアウォールクラスターにおける負荷分散を提供することをさらに実行させるための、項目 2 0～2 2 のいずれか一項に記載のプログラム。

[項目 2 4]

前記コンピュータに、アプリケーション状態データを前記少なくとも 1 つのバックアップノードに提供することと、

前記第 1 のノードの故障に応じて、前記アプリケーション状態データを前記第 2 のノードに提供することと

を更に実行させるための、項目 2 0～2 3 のいずれか一項に記載のプログラム。

[項目 2 5]

3 つ以上のノードを有するファイアウォールクラスターの第 1 のノードによって、パケットに関連付けられた接続情報を処理することと、

接続を確立することと、

前記接続に関連付けられた状態データを前記ファイアウォールクラスター内の少なくとも 1 つのバックアップノードに提供することと、

前記第 1 のノードの故障に応じて、前記接続を前記クラスター内の第 2 のノードに転送することと、

前記状態データを前記バックアップノードから前記第 2 のノードに提供することと

を含む、方法。

[項目 2 6]

前記状態データを、前記ファイアウォールクラスター内の他の複数のノードにブロードキャストすることを更に含む、項目 2 5 に記載の方法。

[項目 2 7]

前記状態データを前記ファイアウォールクラスター内のマスターノードに提供することを更に含む、項目 2 5 又は 2 6 に記載の方法。

[項目 2 8]

別のノードにおいて前記接続をフィルタリングし、前記ファイアウォールクラスターにおける負荷分散を提供することを更に含む、項目 2 5～2 7 のいずれか一項に記載の方法。

[項目 2 9]

アプリケーション状態データを前記少なくとも 1 つのバックアップノードに提供することと、

前記第 1 のノードの故障に応じて、前記アプリケーション状態データを前記第 2 のノードに提供することと

を更に含む、項目 2 5～2 8 のいずれか一項に記載の方法。

[項目 3 0]

3 つ以上のノードを有するファイアウォールクラスターであって、

複数のプロセッサと、

前記複数のプロセッサのうちの 1 以上と通信可能に接続されたメモリとを備え、

前記ファイアウォールクラスター内のそれぞれのノードは、前記複数のプロセッサのうちの 1 以上において動作するべく構成されており、

前記ファイアウォールクラスター内の第 1 のノードは、

パケットに関連付けられた接続情報を処理し、

接続を確立し、

前記接続に関連付けられた状態データを前記ファイアウォールクラスター内の少なくとも 1 つのバックアップノードに提供するように動作可能であり、

前記バックアップノードは、

10

20

30

40

50

前記第 1 のノードの故障に応じて、前記接続を、前記第 1 のノードから前記ファイアウォールクラスター内の第 2 のノードに転送し、

前記状態データを前記第 2 のノードに提供するように動作可能である、ファイアウォールクラスター。

[項目 3 1]

前記第 1 のノードは、前記状態データを、前記ファイアウォールクラスター内の他の複数のノードにブロードキャストするように更に動作可能である、項目 3 0 に記載のファイアウォールクラスター。

[項目 3 2]

前記第 1 のノードは、前記状態データを前記ファイアウォールクラスター内のマスターノードに提供するように更に動作可能である、項目 3 0 又は 3 1 に記載のファイアウォールクラスター。

[項目 3 3]

前記マスターノードは、前記状態データを前記ファイアウォールクラスター内の他の複数のノードにブロードキャストするように動作可能である、項目 3 2 に記載のファイアウォールクラスター。

[項目 3 4]

前記マスターノードは、別のノードにおいて前記接続をフィルタリングし、前記ファイアウォールクラスターにおける負荷分散を提供するように更に動作可能である、項目 3 2 に記載のファイアウォールクラスター。

[項目 3 5]

前記第 1 のノードは、アプリケーション状態データを前記少なくとも 1 つのバックアップノードに提供するように更に動作可能であり、

前記バックアップノードは、前記第 1 のノードの前記故障に応じて、前記アプリケーション状態データを前記第 2 のノードに提供するように更に動作可能である、項目 3 0 ～ 3 4 のいずれか一項に記載のファイアウォールクラスター。

[項目 3 6]

3 つ以上のノードを有するファイアウォールクラスターのノードであって、

1 以上のプロセッサと、

メモリと

を備え、

前記メモリには、実行された場合に、1 以上のプロセッサに、

前記ファイアウォールクラスターの第 1 のノードによって確立された接続に関連付けられた状態データを受信することと、

前記状態データを格納することと、

前記第 1 のノードの故障に応じて、前記接続を前記第 1 のノードから前記ファイアウォールクラスターの第 2 のノードに転送することと、

前記状態データを前記第 2 のノードに提供することと

を実行させるための命令が格納されている、ノード。

[項目 3 7]

前記命令は、実行された場合に、1 以上のプロセッサに、前記状態データを前記ファイアウォールクラスターの他の複数のノードにブロードキャストすることを実行させる命令を更に含む、項目 3 6 に記載のノード。

[項目 3 8]

前記命令は、実行された場合に、1 以上のプロセッサに、前記状態データを前記ファイアウォールクラスター内のマスターノードに提供することを実行させる命令を更に含む、項目 3 6 又は 3 7 に記載のノード。

[項目 3 9]

前記命令は、実行された場合に、1 以上のプロセッサに、別のノードにおいて前記接続をフィルタリングし、前記ファイアウォールクラスターにおける負荷分散を提供すること

10

20

30

40

50

を実行させる命令を更に含む、項目 3 6 ～ 3 8 のいずれか一項に記載のノード。

[項目 4 0]

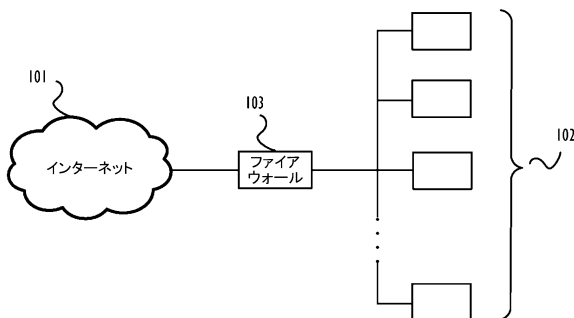
前記命令は、実行された場合に、1 以上のプロセッサに、

アプリケーション状態データを前記第 1 のノードから受信することと、

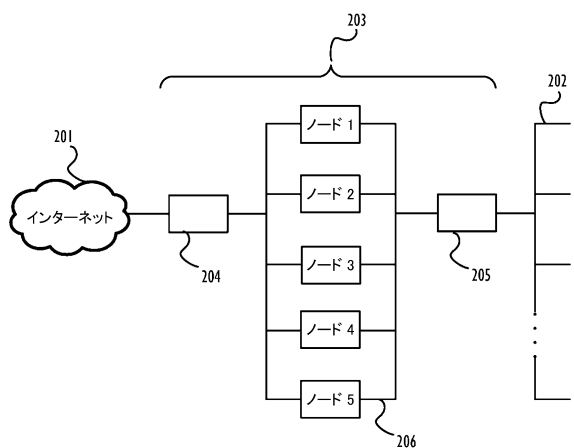
前記第 1 のノードの故障に応じて、前記アプリケーション状態データを前記第 2 のノードに提供することと

を実行させる命令を更に含む、項目 3 6 ～ 3 9 のいずれか一項に記載のノード。

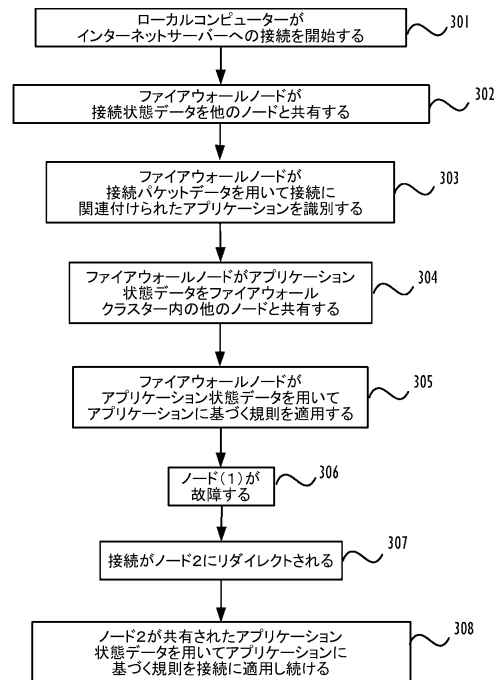
【図 1】



【図 2】



【図 3】



フロントページの続き

(72)発明者 マイヤー、ポール

アメリカ合衆国、95054 カリフォルニア州、サンタ クララ ミッション カレッジ ブー
レバード 2821 マカフィー、インコーポレイテッド内

審査官 大石 博見

(56)参考文献 特開2006-054770 (JP, A)

(58)調査した分野(Int.Cl., DB名)

H04L 12/713

H04L 12/803