

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第7部門第3区分

【発行日】令和3年7月26日(2021.7.26)

【公開番号】特開2021-40352(P2021-40352A)

【公開日】令和3年3月11日(2021.3.11)

【年通号数】公開・登録公報2021-013

【出願番号】特願2020-204851(P2020-204851)

【国際特許分類】

H 0 4 L 12/749 (2013.01)

【F I】

H 0 4 L 12/749

【手続補正書】

【提出日】令和3年5月14日(2021.5.14)

【手続補正1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

分離仮想ネットワークから公にアクセス可能なサービスへのトラフィックをルーティングするためのプライベートエンドポイントを確立するステップと、

前記分離仮想ネットワークから前記公にアクセス可能なサービスに向けられたパケットが、前記プライベートエンドポイントに向けられることを示す1つまたは複数のルーティングテーブルエントリを生成するステップと、

前記1つまたは複数のルーティングテーブルエントリに従って、公衆インターネットを利用せずに、前記分離仮想ネットワークで生じるパケットのコンテンツの少なくとも一部を前記公にアクセス可能なサービスに転送するステップと、
を備える、コンピュータに実装される方法。

【請求項2】

仮想化管理構成要素においてカプセル化パケットを準備するステップであって、前記カプセル化パケットのペイロードは、前記分離仮想ネットワークで生じる前記パケットのコンテンツの少なくとも前記一部を構成する、前記準備するステップと、

前記仮想化管理構成要素から、前記分離仮想ネットワークのトラフィックを処理するように構成された第1の仲介装置に、前記カプセル化パケットを送信するステップと、
をさらに含む、請求項1に記載のコンピュータに実装される方法。

【請求項3】

前記分離仮想ネットワークのトラフィックを処理するように構成された仲介装置において、第1のカプセル化パケットから第2のカプセル化パケットを生成するステップであって、前記第1のカプセル化パケットのペイロードは前記分離仮想ネットワークで生じるパケットのコンテンツの少なくとも前記一部を構成し、前記第1のカプセル化パケットが第1のカプセル化プロトコルに従ってフォーマットされ、前記第2のカプセル化パケットが第2のカプセル化プロトコルに従ってフォーマットされる、前記生成するステップと、

前記第1の仲介装置から、前記第2のカプセル化パケットを、前記第2のカプセル化パケットから前記パケットの前記コンテンツの少なくとも前記一部を抽出するように構成された装置に送信するステップと

を備える、請求項1または2に記載のコンピュータに実装される方法。

【請求項4】

前記プライベートエンドポイントを確立するための1つまたは複数のプログラム要求を取得するステップであって、前記プライベートエンドポイントを確立することは、前記1つまたは複数のプログラム要求への応答である、前記取得するステップ、
をさらに備える、請求項1－3のいずれか1項に記載のコンピュータに実装される方法。

【請求項5】

1つまたは複数のプログラム要求に応答して、前記プライベートエンドポイントを前記公にアクセス可能なサービスに割り当てるステップ、
をさらに備える、請求項1－4のいずれか1項に記載のコンピュータに実装される方法。

【請求項6】

1つまたは複数のプログラム要求に応答して、制御方針を前記プライベートエンドポイントに適用するステップであって、前記制御方針は、前記プライベートエンドポイントを使用してルーティングされた要求に関して、(a)許可された操作タイプ、(b)禁止された操作タイプ、(c)特定の操作タイプが許可される時間間隔、または(d)特定の操作タイプが許可される特定のオブジェクト、のうちの1つまたは複数を示す、
をさらに備える、請求項1－5のいずれか1項に記載のコンピュータに実装される方法。

【請求項7】

他のプライベートエンドポイントを使用するアクセスのための別のサービスを登録するための、1つまたは複数のプログラム要求を取得するステップと、

前記別のサービスを登録する前に、前記別のサービスが前記他のプライベートエンドポイントを介してアクセスするための基準を満たしていることを検証する1つまたは複数の操作を実施するステップと、
をさらに備える、請求項1－6のいずれか1項に記載のコンピュータに実装される方法。

【請求項8】

1つまたは複数のコンピューティングデバイスを備えるシステムであって、
前記1つまたは複数のコンピューティングデバイスは、前記1つまたは複数のコンピューティングデバイス上で、または前記1つまたは複数のコンピューティングデバイス間で実行されると、前記1つまたは複数のコンピューティングデバイスに：

分離仮想ネットワークから公にアクセス可能なサービスへのトラフィックをルーティングするためのプライベートエンドポイントを確立することと、

前記分離仮想ネットワークから前記公にアクセス可能なサービスに向けられたパケットが、前記プライベートエンドポイントに向けられることを示す1つまたは複数のルーティングテーブルエントリを生成することと、

前記1つまたは複数のルーティングテーブルエントリに従って、公衆インターネットを利用せずに、前記分離仮想ネットワークで生じるパケットのコンテンツの少なくとも一部を前記公にアクセス可能なサービスに転送することと、
を行わせる命令を含む、前記システム。

【請求項9】

前記1つまたは複数のコンピューティングデバイスは、前記1つまたは複数のコンピューティングデバイス上で、または前記1つまたは複数のコンピューティングデバイス間で実行されると、前記1つまたは複数のコンピューティングデバイスに：

仮想化管理構成要素においてカプセル化パケットを準備することであって、前記カプセル化パケットのペイロードは、前記分離仮想ネットワークで生じる前記パケットのコンテンツの少なくとも前記一部を構成する、前記準備することと

前記仮想化管理構成要素から、前記分離仮想ネットワークのトラフィックを処理するように構成された第1の仲介装置に、前記カプセル化パケットを送信することと、
を行わせる命令を含む、請求項8に記載のシステム。

【請求項10】

前記1つまたは複数のコンピューティングデバイスは、前記1つまたは複数のコンピューティングデバイス上で、または前記1つまたは複数のコンピューティングデバイス間で実行されると、前記1つまたは複数のコンピューティングデバイスに：

前記分離仮想ネットワークのトラフィックを処理するように構成された仲介装置において、第1のカプセル化パケットから第2のカプセル化パケットを生成することであって、前記第1のカプセル化パケットのペイロードは前記分離仮想ネットワークで生じるパケットのコンテンツの少なくとも一部を構成し、前記第1のカプセル化パケットが前記第1のカプセル化プロトコルに従ってフォーマットされ、前記第2のカプセル化パケットが第2のカプセル化プロトコルに従ってフォーマットされる、前記生成することと、

前記第2のカプセル化パケットを、前記第1の仲介装置から、前記第2のカプセル化パケットから前記パケットの内容の少なくとも一部を抽出するように構成された装置に送信すること、

を行わせる命令をさらに含む、請求項8または請求項9に記載のシステム。

【請求項11】

前記1つまたは複数のコンピューティングデバイスは、前記1つまたは複数のコンピューティングデバイス上で、または前記1つまたは複数のコンピューティングデバイス間で実行されると、前記1つまたは複数のコンピューティングデバイスに：

プライベートエンドポイントを確立するための1つまたは複数のプログラム要求を取得することであって、前記プライベートエンドポイントは、前記1つまたは複数のプログラム要求に応じて確立される、前記取得すること

を行わせる命令をさらに含む、請求項8－10のいずれか1項に記載のシステム。

【請求項12】

前記1つまたは複数のコンピューティングデバイスは、前記1つまたは複数のコンピューティングデバイス上で、または前記1つまたは複数のコンピューティングデバイス間で実行されると、前記1つまたは複数のコンピューティングデバイスに：

1つまたは複数のプログラム要求に応じて、プライベートエンドポイントを公的にアクセス可能なサービスに割り当てること、

を行わせる命令をさらに含む、請求項8－11のいずれか1項に記載のシステム。

【請求項13】

前記1つまたは複数のコンピューティングデバイスは、前記1つまたは複数のコンピューティングデバイス上で、または前記1つまたは複数のコンピューティングデバイス間で実行されると、前記1つまたは複数のコンピューティングデバイスに：

1つまたは複数のプログラム要求にตอบสนองして、プライベートエンドポイントに制御方針を適用することであって、前記制御方針は、プライベートエンドポイントを使用してルーティングされた要求に関して、(a)許可された操作タイプ、(b)禁止された操作タイプ、(c)特定の操作タイプが許可される時間間隔、または(d)特定の操作タイプが許可される特定のオブジェクト、のうちの1つまたは複数を示す、前記適用すること、

を行わせる命令をさらに含む、請求項8－12のいずれか1項に記載のシステム。

【請求項14】

前記1つまたは複数のコンピューティングデバイスは、前記1つまたは複数のコンピューティングデバイス上で、または前記1つまたは複数のコンピューティングデバイス間で実行されると、前記1つまたは複数のコンピューティングデバイスに：

前記分離仮想ネットワークで生じるパケットのコンテンツの一部を、トンネリングプロトコルを使用して、前記公にアクセス可能なサービスに転送すること、

を行わせる命令をさらに含む、請求項8－13のいずれか1項に記載のシステム。

【請求項15】

プログラム命令を格納した1つまたは複数のコンピュータアクセス可能な記憶媒体であって、前記プログラム命令は、1つまたは複数のプロセッサ上で実行されると、前記1つまたは複数のプロセッサに：

分離仮想ネットワークから公にアクセス可能なサービスへのトラフィックをルーティングするためのプライベートエンドポイントを確立することと、

前記分離仮想ネットワークから前記公にアクセス可能なサービスに向けられたパケットが、前記プライベートエンドポイントに向けられることを示す1つまたは複数のルーティ

ングテーブルエントリを生成することと、

前記1つまたは複数のルーティングテーブルエントリに従って、公衆インターネットを利用せずに、前記分離仮想ネットワークで生じるパケットのコンテンツの少なくとも一部を前記公にアクセス可能なサービスに転送することと、
を実行させる、コンピュータアクセス可能な記憶媒体。