(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 715 223**

(51) Int. CI.:

G06Q 20/10 (2012.01)
G06Q 20/34 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.07.2011 PCT/US2011/044530**

(87) Fecha y número de publicación internacional: **26.01.2012 WO12012421**

(96) Fecha de presentación y número de la solicitud europea: **19.07.2011 E 11810277 (1)**

(97) Fecha y número de publicación de la concesión europea: **26.12.2018 EP 2596466**

(54) Título: **Sistema y método para emisión instantánea de tarjetas de transacción financieras personalizadas**

(30) Prioridad:

19.07.2010 US 365673 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.06.2019

(73) Titular/es:

CPI CARD GROUP - TENNESSEE, INC. (100.0%)
556 Metroplex Drive
Nashville, Tennessee 37211, US

(72) Inventor/es:

SMITH, BOBBY y
WHITE, JAMES

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Sistema y método para emisión instantánea de tarjetas de transacción financieras personalizadas

Campo técnico

La presente invención se refiere a métodos y sistemas para crear, emitir e imprimir tarjetas de transacción financiera, tales como tarjetas de crédito emitidas a clientes por instituciones financieras.

Más específicamente, la presente invención pertenece a métodos y sistemas que permiten que un banco u otra institución financiera emitan de manera instantánea y segura una tarjeta de crédito personalizada a un cliente en una sucursal u otra localización remota.

Antecedentes de la técnica

Muchas cuentas de nuevos clientes abiertas por bancos incluyen una o más tarjetas de débito o de crédito asociadas con la cuenta. Las nuevas cuentas de cliente se abren típicamente en localizaciones de sucursal mientras que las nuevas tarjetas a menudo se emiten por un proveedor de servicios de tarjeta centralizado que no está físicamente cerca de la sucursal bancaria. Por consiguiente, el cliente debe suministrar información de tarjeta a un empleado de banca en la sucursal. El cliente puede tener o no una oportunidad para seleccionar un PIN personalizado en ese momento. Estos datos de tarjeta a continuación se comunican, tal vez en un modo por lotes con otros datos de tarjeta, a un proveedor de servicios de tarjeta.

El proveedor de servicios de tarjeta cumple con la solicitud de tarjeta imprimiendo y codificando la tarjeta, enviándola por correo a continuación a la sucursal o al cliente. El cliente debe a continuación activar la tarjeta. Este proceso implica retardo y coste que son indeseables y pueden introducir riesgos de seguridad innecesarios.

Lo que es necesario, entonces, es un sistema y método de bajo coste, seguro, sencillo y fácil de instalar para proporcionar emisión instantánea de tarjetas de transacción financiera personalizadas en una sucursal bancaria. Este sistema y método necesarios deberían interconectar con la nueva plataforma/anfitrión de cuentas por el banco y cumplir todos los requisitos de seguridad impuestos por los principales emisores de tarjeta de crédito y débito y procesadores de transacciones. El documento US 2010/0123003 A1 desvela

- Un método para emitir una tarjeta de transacción financiera personalizada de una institución financiera a un cliente en respuesta a una solicitud de cliente realizada desde una localización de cliente,
- en el que la solicitud de cliente incluye información de cliente asociada con el cliente e información de tarjeta a asociarse con la tarjeta de transacción financiera, comprendiendo el método:
- comunicar electrónicamente la información de cliente a través de una red de datos a una red de proveedor de servicios de tarjeta;
- introducir electrónicamente la información de cliente comunicada a la red de proveedor de servicios de tarjeta en una base de datos;
- usar software de aplicación asociado con la base de datos,
- generar un número de tarjeta asociado con el cliente y un PIN;
- almacenar el número de tarjeta y al menos uno de la información de cliente en un fichero de tarjeta electrónica asociado con el cliente;
- usar el software de aplicación para aplicar cálculos al PIN para generar un código de verificación;
- enviar de manera segura el número de tarjeta y código de verificación del proveedor de servicios de tarjeta a través de la red de datos a la localización de cliente, e
- imprimir la tarjeta de transacción financiera con el miembro de tarjeta y código de verificación para el cliente en la localización de cliente.

Adicionalmente, los documentos WO 2006/056826 A1 y US 2005/240994 A1 se citan como la técnica anterior relacionada.

Divulgación de la invención

La presente invención es un método de acuerdo con la reivindicación 1, para emitir una tarjeta de transacción financiera personalizada de una institución financiera a un cliente en respuesta a una solicitud de cliente realizada desde una localización de sucursal asociada con la institución financiera. Un empleado u operador de banca recibe información de cliente e información de tarjeta del cliente en la localización de la sucursal. La información de tarjeta puede incluir un número de identificación personal (PIN) de la tarjeta. El operador introduce la información de cliente y al menos alguna de la información de tarjeta en un terminal de procesamiento de datos en la sucursal.

La información de cliente y la información de tarjeta se comunican desde la sucursal a través de una red a un proveedor de servicios de tarjeta. En el proveedor de servicios de tarjeta, se introduce el PIN en una base de datos de PIN, se genera un número de referencia asociado con el cliente, y se genera una validación de PIN. El número de referencia

y al menos uno de los datos de cliente y datos de tarjeta pueden almacenarse en un fichero de tarjeta asociado con el cliente. El número de referencia se usa para recuperar el PIN de la base de datos de PIN. El PIN recuperado se usa a continuación para aplicar cálculos al fichero de tarjeta.

El fichero de tarjeta se envía de manera segura desde el proveedor de servicios de tarjeta a través de la red a la localización de la sucursal. Usando información desde el fichero de tarjeta, se imprime la tarjeta de transacción financiera para el cliente en la localización de la sucursal. En una realización preferida, la tarjeta personalizada se emite instantáneamente mientras el cliente está presente en la localización de la sucursal.

En una realización, puede enviarse un mensaje de verificación a la institución financiera y a un procesador de transacción de tarjeta cuando se ha impreso satisfactoriamente la tarjeta de transacción financiera. También, puede enviarse un mensaje de error a la localización de la sucursal y a un procesador de transacción de tarjeta cuando la tarjeta de transacción financiera no se ha impreso satisfactoriamente.

En una realización adicional del método, la etapa de enviar de manera segura el fichero de tarjeta a la localización de la sucursal puede incluir distribuir un escritorio virtual desde un servidor en el proveedor de servicios de tarjeta a través de la red a un cliente de escritorio virtual en la localización de la sucursal.

En algunas realizaciones, el fichero de tarjeta puede almacenarse en la localización de la sucursal y la etapa de almacenamiento del número de referencia y al menos uno de los datos de cliente puede incluir adicionalmente actualizar el fichero de tarjeta con el número de referencia en la localización de la sucursal.

En otra realización más de la invención, después de que se actualiza el fichero de tarjeta en la localización de la sucursal con el número de referencia, el método puede incluir enviar una solicitud de emisión de tarjeta desde la localización de la sucursal y recibirla en un módulo de seguridad de hardware (HSM) en el proveedor de servicios de tarjeta. En esta realización, en respuesta a recibir la solicitud de emisión de tarjeta, el HSM puede recuperar el PIN de la base de datos de PIN y aplicar el número de referencia a los cálculos en el fichero de tarjeta.

Por lo tanto, el sistema y método de la presente invención minimizarán costes por adelantado incurridos por bancos de institución financiera para las cuotas de hardware, software, licencia y mantenimiento. Proporcionará un proceso seguro para PIN seleccionados de cliente y estará basado en aplicaciones de servicio web seguras para transmitir datos de personalización de tarjeta para controlar las impresoras de tarjeta remotas.

Breve descripción de los dibujos

La Figura 1(a) es un diagrama de bloques que muestra una disposición de hardware y módulos de software de acuerdo con una realización del sistema de la presente invención, que muestra adicionalmente comunicaciones de sistema desde un PC de sobremesa de sucursal bancaria que comunica una solicitud de emisión de tarjeta instantánea al servicio web de sistema.

La Figura 1(b) es un diagrama de bloques del sistema de la Figura 1(a), que muestra adicionalmente comunicaciones de sistema entre el servicio web de sistema y el servicio web de proveedor de servicios de tarjeta después de la iniciación de la solicitud de emisión instantánea como se muestra en la Figura 1(a).

La Figura 1(c) es un diagrama de bloques del sistema de la Figura 1(a), que muestra adicionalmente comunicaciones de sistema entre el servicio web de proveedor de servicios de tarjeta y el servidor de aplicación de proveedor de servicios de tarjeta después de la iniciación de la solicitud de emisión instantánea como se muestra en las Figuras 1(a) y 1(b).

La Figura 1(d) es un diagrama de bloques del sistema de la Figura 1(a), que muestra adicionalmente el servidor de aplicación de proveedor de servicios de tarjeta que pone datos en un servidor de base de datos de proveedor de servicios de tarjeta después de la iniciación de la solicitud de emisión instantánea como se muestra en las Figuras 1(a)-1(c).

La Figura 1(e) es un diagrama de bloques del sistema de la Figura 1(a), que muestra adicionalmente el servidor de aplicación de proveedor de servicios de tarjeta que recupera un cálculo de PIN/validación desde el módulo de seguridad de hardware de proveedor de servicios de tarjeta después de la iniciación de la solicitud de emisión instantánea como se muestra en las Figuras 1(a)-1(d).

La Figura 1(f) es un diagrama de bloques del sistema de la Figura 1(a), que muestra adicionalmente el servidor de aplicación de proveedor de servicios de tarjeta que comunica un trabajo de impresión de tarjetas al servidor de impresión de proveedor de servicios de tarjeta después de la iniciación de la solicitud de emisión instantánea como se muestra en las Figuras 1(a)-1(e).

La Figura 1(g) es un diagrama de bloques del sistema de la Figura 1(a), que muestra adicionalmente el servidor de impresión de proveedor de servicios de tarjeta que comunica de manera segura un trabajo de impresión de tarjetas a una impresora en la sucursal bancaria, después de la iniciación de la solicitud de emisión instantánea como se muestra en las Figuras 1(a)-1(f).

La Figura 1(h) es un diagrama de bloques del sistema de la Figura 1(a), que muestra adicionalmente la impresora en la sucursal bancaria que comunica un mensaje de éxito o fallo de trabajo de impresión de tarjetas de vuelta al servidor de impresión de proveedor de servicios de tarjeta, después de la iniciación de la solicitud de emisión instantánea como se muestra en las Figuras 1(a)-1(g).

La Figura 1(i) es un diagrama de bloques del sistema de la Figura 1(a), que muestra adicionalmente el servidor de impresión de proveedor de servicios de tarjeta que comunica un mensaje de éxito o fallo de trabajo de impresión de tarjetas de vuelta al servidor de aplicación de proveedor de servicios de tarjeta, después de la iniciación de la solicitud de emisión instantánea como se muestra en las Figuras 1(a)-1(h).

La Figura 1(j) es un diagrama de bloques del sistema de la Figura 1(a), que muestra adicionalmente el servidor de aplicación de proveedor de servicios de tarjeta que publica información de éxito o fallo de impresión de tarjetas al servicio web de sistema, después de la iniciación de la solicitud de emisión instantánea como se muestra en las Figuras 1(a)-1(i).

La Figura 1(k) es un diagrama de bloques del sistema de la Figura 1(a), que muestra adicionalmente el servicio web de sistema que comunica información de éxito o fallo de impresión de tarjetas al PC de sobremesa de sucursal bancaria, después de la iniciación de la solicitud de emisión instantánea como se muestra en las Figuras 1(a)-1(j).

La Figura 2 es un diagrama de flujo que ilustra un método para emisión instantánea de una tarjeta de crédito personalizada en una sucursal bancaria, de acuerdo con una realización de la presente invención.

La Figura 3a es un diagrama de bloques que muestra una disposición de hardware y módulos de software de acuerdo con otra realización del sistema de la presente invención.

La Figura 3b es un diagrama de bloques de la realización del sistema de la Figura 3a, que muestra adicionalmente un túnel de VPN de sitio a sitio que se establece entre el servicio web de sistema y el servicio web de proveedor de servicios de tarjeta.

La Figura 3c es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente un túnel de VPN de sitio a sitio dinámico creado entre la impresora y dispositivo de impresora y la red DMZ de impresión.

La Figura 3d es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente una conexión persistente entre el servidor de impresión al servidor de aplicación.

La Figura 3e es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente la sucursal bancaria que emite una solicitud de emisión instantánea de tarjeta al servicio web de sistema.

La Figura 3f es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente el servicio web de sistema que envía una solicitud HTTP POST a la red DMZ de servicio web.

La Figura 3 g es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente el HTTP POST que se envía al servidor de aplicación de proveedor de servicios de tarjeta compatible con PCI y el estado de HTTP que se devuelve al servicio web.

La Figura 3h es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente el servidor 50a de aplicación compatible con PCI que solicita un Criptograma de Clave CW de tarjeta desde el servidor 50b de aplicación.

La Figura 3i es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente el servidor de aplicación que envía la solicitud de impresión de tarjetas a la base de datos de proveedor de servicios de tarjeta y que devuelve los resultados al servidor de aplicación.

La Figura 3j es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente el servidor de aplicación que comunica al módulo de seguridad de hardware, que envía el Criptograma o Criptogramas de Clave CVV y datos de personalización de tarjeta, y que recupera los valores CV1 y CV2.

La Figura 3k es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente el servidor 50a de aplicación compatible con PCI que entra en contacto con el servidor 50b de aplicación y que solicita información de cálculo de imagen de tarjeta.

La Figura 3l es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente el servidor de aplicación que recupera la información de cálculo de imagen de tarjeta desde la base de datos y que devuelve los resultados.

La Figura 3m es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente el servidor 50a de aplicación que conecta al servidor 50b de aplicación y que solicita los datos de imagen de tarjeta.

La Figura 3n es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente el servidor 50b de aplicación que recupera los datos de imagen de tarjeta desde el servidor de ficheros y que los transmite de vuelta a través de la solicitud de HTTP.

La Figura 3o es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente el servidor 50a de aplicación que conecta al servidor 50b de aplicación para recuperar datos de cálculo de banda magnética de tarjeta.

La Figura 3p es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente el servidor 50b de aplicación que recupera los datos de cálculo de banda magnética desde la base de datos y que devuelve los resultados al servidor 50a de aplicación a través de la respuesta de HTTP.

La Figura 3q es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente el servidor 50a de aplicación que comunica el trabajo de impresión de tarjetas en un bus de mensaje de trabajo de impresión.

La Figura 3r es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente un agente de conexión que asigna el trabajo de impresión a un subproceso de trabajador en el servidor de impresión.

La Figura 3s es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente el servidor de impresión que envía el trabajo de impresión a la impresora a través del túnel de VPN de sitio a sitio dinámico.

La Figura 3t es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente la impresora que intenta imprimir la tarjeta y que envía un mensaje de respuesta de impresión de tarjetas (éxito/fallo/intervención de usuario requerida) de vuelta al servidor de impresión.

La Figura 3u es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente el subproceso del trabajador que pone el resultado de impresión en el bus de mensaje.

La Figura 3v es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente el servidor de aplicación que envía el resultado de impresión a la red DMZ de servicio web mediante HTTP POST.
La Figura 3w es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente el servidor de intermediario en el servicio web de proveedor de servicios de tarjeta que retransmite el resultado de impresión de tarjetas al servicio web de sistema.
La Figura 3x es un diagrama de bloques del sistema de la Figura 3a, que muestra adicionalmente el servicio web de sistema que retransmite el resultado de impresión de tarjetas a la sucursal de banco solicitante.

Mejor modo para llevar a cabo la invención

Haciendo referencia ahora a las Figuras 1(a)-(k), se muestra una disposición de elementos, componentes y módulos de hardware y software, usados en una realización del sistema 10 de la presente invención. En esta realización, un banco proporciona servicios de banca minorista a clientes a través de una o más sucursales 15a-15c de banca. Las sucursales 15 ejecutan sistemas de procesamiento de datos conectados entre sí y a una oficina central de banco por una red de área extensa (WLAN) o servicio 20 web de sistema y una red 5 de datos pública, tal como la Internet pública.

Convencionalmente, el banco y sus sucursales 15 están autorizados para emitir tarjetas de transacción financiera, tales como tarjetas de débito o de crédito, que están asociadas con un procesador de transacción de tarjeta de marca tal como Visa® o MasterCard®. Estos procesadores de transacciones operan y controlan una red financiera global de emisores, adquirientes, comerciantes de tarjeta interconectados electrónicamente y centros de procesamiento de datos.

El banco puede contratar con un proveedor de servicios de tarjeta para proporcionar servicios asociados con la emisión de una nueva tarjeta de crédito o de débito a un cliente de banca. En la realización de la Figura 1(a), el proveedor de servicios de tarjeta operará redes 35 de hardware y software que pueden recibir y procesar solicitudes de nuevas tarjetas enviadas por una sucursal 15 bancaria. Las redes de proveedor de servicio de tarjeta pueden incluir una red 55 DMZ de servicio web de emisión instantánea, una red 36 de servidor de emisión instantánea, una red 45 de personalización de emisión instantánea, y una red 60 DMZ de impresión de emisión instantánea.

La red 36 de servidor de emisión instantánea puede incluir un directorio activo o controlador 37 de dominio, un servidor 50 de aplicación, y un servidor 41 de base de datos. Por consiguiente, el proveedor de servicios de tarjeta mantendrá una base de datos 40 de PIN (Número de Identificación Personal) conectada al servidor 41 de base de datos que puede almacenar de manera segura PIN seleccionados por clientes de banca cuando se emite una nueva tarjeta.

Como parte de la red 45 de personalización de emisión instantánea, el proveedor de servicios de tarjeta puede operar también un módulo de seguridad de hardware-anfitrión (HSM) 47 para proporcionar un entorno seguro para encriptación de datos de tarjeta, cálculos de PIN, operaciones criptográficas sensibles, almacenamiento de clave segura, y gestión de un gran número de claves seguras, como es conocido para un experto en la materia. Un módulo de seguridad de hardware-anfitrión, como se conoce por los expertos en la materia, es una combinación de hardware y software/firmware que está conectado funcionalmente a un PC o servidor para proporcionar funciones criptográficas. El HSM 47 puede incluir una interfaz de usuario e interfaz programable. La parte física de un HSM, que puede ser una tarjeta de módulo de extensión o dispositivo externo tal como un Servidor Windows físico, puede incluir características resistentes a la manipulación.

Preferentemente, la interfaz funcional entre las redes 35 de proveedor de servicio de tarjeta, la red 5 pública, y el servicio 20 web de sistema puede incluir una red 55 de "zona desmilitarizada" (DMZ) de servicio web. Una zona desmilitarizada, en ocasiones denominada como una Red Perimetral, es una subred física o lógica que contiene y expone unos servicios externos de la organización a una red no confiable mayor, tal como Internet. La red 55 DMZ añade una capa adicional de seguridad al enlace de comunicaciones entre el servicio 20 web de sistema y las redes 35 de proveedor de servicio de tarjeta, de modo que un atacante externo tiene acceso únicamente al hardware en la DMZ y no en ninguna otra parte de las redes. Dentro de la red 55 DMZ se encuentra un servicio 56 web de proveedor de servicios de tarjeta. El servicio web 56 puede implementarse usando, por ejemplo, un servidor virtual Windows o servidor de intermediario Apache.

La red 55 DMZ y el servicio 20 web de sistema pueden interconectarse por una conexión de red privada o a través de la red 5 pública, tal como la Internet pública. En una realización, esta conexión puede implementarse por un túnel de Red Privada Virtual (VPN) encriptado (por ejemplo, IPSEC) usando un dispositivo de punto terminal de IPSEC o aparato 59 de seguridad. Un ejemplo convencional de aparato de seguridad que puede usarse es un Cortafuegos Modelo ASA 5050 de Cisco Systems, Inc. La red 36 de servidor de emisión instantánea puede acoplarse a la red 55 DMZ a través de un cortafuegos 58, por ejemplo, un aparato virtual. El HSM 47 está también acoplado de manera funcional a la red 36 de servidor de emisión instantánea usando un cortafuegos 46, por ejemplo, un aparato virtual.

Las redes 35 de proveedor de servicios de tarjeta pueden incluir una red 60 DMZ de impresión de tarjetas de emisión instantánea que contiene un servidor 61 de impresión. La red 60 DMZ de impresión de tarjetas de emisión instantánea puede estar conectada a la red 55 DMZ a través de un cortafuegos 38, por ejemplo, un aparato de seguridad tal como

el Cortafuegos Cisco ASA 5050. La red 60 DMZ de impresión de tarjetas de emisión instantánea y el servicio 20 web de sistema pueden estar interconectados por una conexión de red privada o a través de la red 5 pública. En una realización, esta conexión puede implementarse usando un túnel de Red Privada Virtual (VPN) encriptado (por ejemplo, IPSEC) y un dispositivo 62 de punto terminal de IPSEC tal como el Cortafuegos Cisco ASA 5050.

El sistema 10 puede incluir también hardware y software localizado en cada localización 15 de sucursal, que incluye uno o más PC de sobremesa o estaciones de trabajo 16 funcionalmente acoplados al servicio 20 web de sistema y una red 17 de impresora de tarjetas de sucursal. En una realización, la red 17 de impresora de tarjetas de sucursal incluye una impresora 18 de tarjetas. La red 17 de impresora de tarjetas de sucursal puede aislarse y por lo tanto acoplarse a la red 60 DMZ de impresión de tarjetas de emisión instantánea usando un túnel VPN establecido entre un cortafuegos y el dispositivo de punto terminal de IPSEC y el dispositivo 62 de punto terminal. La red 17 de impresora de tarjetas de sucursal puede también estar conectada a la red 5 pública a través del cortafuegos y el dispositivo 19 de punto terminal de IPSEC. En la realización mostrada, se usa una conexión a Internet inalámbrica. En una realización, la impresora 18 de tarjetas puede ser una Impresora de Tarjetas Financieras Datacard Modelo FP65i de Datacard Group.

En la realización de las Figuras 1(a)-(k), los PC 16 de sobremesa de sucursal pueden comunicar de manera segura con las redes 35 de proveedor de servicio de tarjeta. Los PC 16 de sucursal accederán y visualizarán una o más interfaces de usuario de sistema basado en explorador generadas por el servicio 20 web de sistema y el servicio 56 web de proveedor de servicios. Esta interfaz de usuario en los PC 16 de sucursal se usa por un operador de banca en la sucursal durante el proceso de usar el sistema 10 para solicitar y emitir una nueva tarjeta. Los PC 16 de sobremesa están acoplados funcionalmente a las redes 35 de proveedor de servicios de cliente a través del servicio 20 web de sistema y a la red 55 DMZ para proporcionar comunicaciones de datos seguras entre las sucursales 15 y las redes de proveedor de servicio de tarjeta.

La impresora 18 de tarjetas de sucursal está acoplada funcionalmente al servidor 61 de impresión de proveedor de servicios de cliente para recibir de manera segura comandos de impresión de tarjetas. La impresora 18 de tarjetas puede equiparse con un suministro de existencias de tarjetas en blanco. La impresora 18 de tarjetas usa los datos en un fichero de tarjetas para imprimir una tarjeta en blanco con información personalizada asociada con y seleccionada por un cliente.

Haciendo referencia ahora a la Figura 2, puede describirse una realización de un método 100 para emisión instantánea de una tarjeta de crédito personalizada a un cliente de banca localizado en una localización de sucursal bancaria. En una primera etapa 110, un empleado de banca u otro operador de sistema que trabaja en la sucursal recibe información del cliente que es necesaria para iniciar la solicitud para emisión de una tarjeta de crédito o débito personalizada para el cliente. Esta información se introduce en correspondientes campos de datos de tarjeta usados por el sistema. En una realización los campos de datos de tarjeta son parte de un fichero de tarjeta CAF. Los campos de datos en el fichero de tarjeta pueden incluir datos que identifican el nombre y dirección de cliente, la sucursal, el operador de banca, y el tipo particular de tarjeta de transacción financiera (por ejemplo, crédito o débito) que se está solicitando.

En una segunda etapa 120, el cliente selecciona un PIN (Número de Identificación Personal) que estará asociado con la tarjeta a emitirse al cliente. En una realización preferida, el PIN personalizado se introduce en el sistema por el cliente directamente, usando un terminal de datos de tipo teclado numérico en la sucursal o un teléfono y sistema de reconocimiento de voz, de modo que el operador de banca no observa o escucha el PIN. Un sistema de selección de PIN que puede usarse para este fin se describe en la Patente de Estados Unidos N. º 5.132.521, la divulgación total de la cual se incorpora en el presente documento por referencia.

El PIN seleccionado se comunica electrónicamente 130 a una base de datos de PIN. En una realización, la base de datos de PIN se mantiene de manera remota por una compañía de servicios de tarjeta que tiene un contrato con el banco para producir, codificar y emitir tarjetas de transacción financiera personalizadas a clientes de ese banco.

En una cuarta etapa 140, el software asociado con la base de datos de PIN genera un número de referencia asociado con el cliente y el PIN seleccionado. El número de referencia se comunica a y puede almacenarse en el fichero de tarjeta asociado con el cliente como una actualización de fichero. Este fichero de tarjeta actualizado puede usarse por el sistema software usado en la localización de la sucursal.

En una realización del método, después de que se actualiza el fichero de tarjeta después de la generación del número de referencia, se comunica 150 una solicitud de tarjeta a una aplicación de software de función de edición en el módulo de seguridad de anfitrión de hardware (HSM) 47. El HSM 47 puede controlarse por un proveedor de servicios de tarjeta remoto de la sucursal. La aplicación de función de edición de HSM usa el número de referencia para recuperar 160 el PIN de la base de datos de PIN de modo que pueden aplicarse cálculos algorítmicos al PIN en el fichero de tarjeta.
En una siguiente etapa 170, el fichero de tarjeta se envía de manera segura a una impresora de tarjetas remota en la localización de la sucursal. En una realización, esta etapa se implementa por medio de un servidor de escritorio virtual que comunica con un cliente de escritorio virtual asociado con la impresora de tarjetas remota y un PC o terminal localizado en la sucursal.

La tarjeta del cliente a continuación se imprime 180 por la impresora remota usando los datos en el fichero de tarjeta. Después de que se imprime la tarjeta, puede enviarse 190 un mensaje de verificación al banco y al procesador de transacción de la tarjeta. Este mensaje de verificación confirma que la tarjeta ya está lista para su uso por el cliente. Como alternativa, si la impresión de tarjetas no es satisfactoria, se comunica 200 un mensaje de error al operador de banca en la sucursal y al procesador de transacción.

Una realización de un método para emisión instantánea de una tarjeta de crédito personalizada a un cliente de banca localizado en una localización de sucursal bancaria puede entenderse adicionalmente por referencia a las Figuras 1(a)-1 (k). Para iniciar el proceso como se muestra en la Figura 1(a), un operador de sistema hace una solicitud de emisión de tarjeta en el PC 16 de sobremesa de sucursal, que a continuación comunica una solicitud de emisión de tarjeta instantánea al servicio 20 web de sistema.

El servicio 20 web de sistema conecta al servicio 56 web de proveedor de servicios de tarjeta a través de un túnel seguro persistente (por ejemplo, IPSEC) y comunica la solicitud de emisión instantánea de tarjeta a las redes 35 de proveedor de servicios de cliente, como se muestra en la Figura 1(b). El servicio 56 web de proveedor de servicios de tarjeta conecta al servidor 50 de aplicación de proveedor de servicios de tarjeta (Figura 1(c)). En respuesta, el servidor 50 de aplicación pone datos en la base de datos 40 de proveedor de servicios de tarjeta (Figura 1(d)). Como se muestra en la Figura 1(e), el servidor 50 de aplicación de proveedor de servicios de tarjeta a continuación recupera un cálculo de PIN/validación desde el módulo 47 de seguridad de hardware de proveedor de servicios de tarjeta.

El servidor 50 de aplicación de proveedor de servicios de tarjeta comunica un trabajo de impresión de tarjetas al servidor 61 de impresión de proveedor de servicios de tarjeta, como se observa en la Figura 1(f). Este trabajo de impresión de tarjetas se envía a la impresora 18 de tarjetas de emisión instantánea (Figura 1 (g)). Esto permite que la tarjeta de transacción financiera se imprima en la sucursal 15 bancaria que realizó la solicitud de emisión de tarjeta.

La impresora 18 comunica un mensaje de éxito o fallo de trabajo de impresión de tarjetas de vuelta al servidor 61 de impresión de proveedor de servicios de tarjeta (Figura 1(h)). El servidor 61 de impresión de proveedor de servicios de tarjeta a continuación comunica un mensaje de éxito o fallo de trabajo de impresión de tarjetas de vuelta al servidor 50 de aplicación de proveedor de servicios de tarjeta (Figura 1(i)). El servidor 50 de aplicación de proveedor de servicios de tarjeta a continuación publica información de éxito o fallo de impresión de tarjetas al servicio 20 web de sistema ((Figura 1(j)). Finalmente, como se muestra en la Figura 1(k), el servicio 20 web de sistema comunica información de éxito o fallo de impresión de tarjetas al PC 16 de sobremesa de sucursal bancaria.

La Figura 3a ilustra otra realización del sistema 10 en la que la impresora 18 de tarjetas en la localización de la sucursal 15 está combinada físicamente con un aparato 21 de seguridad dentro de un alojamiento común. En esta realización, la combinación de la impresora 18 de tarjetas y el aparato 21 de seguridad puede ser compatible con PCI (Industria de Tarjetas de Pago). Esta compatibilidad requiere un método novedoso para gestionar un túnel de IPSEC a través de un aparato 21 de Linux.

Existen varias técnicas conocidas para negociar un túnel de IPSEC. Una técnica común es usar una clave pre-compartida (PSK) compartida entre dos direcciones IP estáticas públicas. Este tipo de túnel permite que cualquier extremo inicie el túnel cuando se detecte el tráfico designado para el otro extremo del túnel. Este tráfico es conocido en la técnica como "tráfico interesante". Cuando no hay "tráfico interesante" (durante un periodo de tiempo preconfigurado) la asociación de seguridad entre los puntos terminales se terminará y por lo tanto se dice que el túnel de IPSEC está "caído". Esto no es un problema para dos direcciones de IP estáticas públicas, ya que cualquier lado puede iniciar el túnel a la dirección pública en el extremo remoto. Sin embargo, cuando un lado del túnel no sea estático, o la dirección de IP no sea conocida, o si está detrás de un encaminador/cortafuegos que no es de Traducción de Dirección de Red (NAT), únicamente un extremo (el extremo no estático no público) puede iniciar el túnel de IPSEC. Para que el extremo estático público (el que no inicia) del túnel envíe tráfico al extremo privado dinámico el túnel debe mantenerse de manera agresiva "activo" en todo momento. Para conseguir esto, la realización del sistema mostrado en la Figura 3 incluye un dispositivo con un sistema operativo integrado en la carcasa de la impresora. Este aparato 21 de Linux integrado en el extremo privado dinámico (en la sucursal bancaria) puede iniciar el túnel IPSEC mientras monitoriza el otro lado para conectividad. Si la monitorización detecta problemas, el dispositivo 21 puede restablecer el túnel IPSEC. Por lo tanto, el aparato 21 puede ser un aparato de Linux reforzado que funciona como un encaminador, firewall, y punto terminal de IPSEC de dinámico a estático que cumple con normas del Centro para la Seguridad de Internet (CIS). En esta realización, la impresora 18 de tarjetas puede ser una impresora de tarjetas Dualys de Evolis.

En la realización de la Figura 3a, el proveedor de servicios de tarjeta operará redes 35a y 35b de hardware y software que pueden recibir y procesar solicitudes de nuevas tarjetas enviadas por una sucursal 15 bancaria. Las redes 35a son compatibles con PCI e incluyen una red 55 DMZ de servicio web de emisión instantánea, una red 36a de servidor de emisión instantánea, una red 45 de personalización de emisión instantánea, y una red 60 DMZ de impresión de emisión instantánea, como se ha descrito con referencia a la Figura 1(a).

La red 36a de servidor de emisión instantánea compatible con PCI puede incluir un directorio activo o controlador 37 de dominio, un servidor 50a de aplicación, una o más estaciones de trabajo 39, y un servidor 43 administrativo de IPSEC.

La red 36b de proveedor de servicios de tarjeta incluye un servidor 50b de aplicación, una base de datos 40 de PIN conectada a un servidor 41 de base de datos para almacenar de manera segura PIN seleccionados por clientes de banca cuando se emite una nueva tarjeta, y un servidor 42 de ficheros.

Las Figuras 3a-3x ilustran operación secuencial de esta realización del sistema 10. En la Figura 3b, se establece un enlace de VPN de sitio a sitio entre el servicio 20 web de sistema y las redes 35a y 35b de proveedor de servicio de tarjeta. A continuación se crea un túnel de VPN de sitio a sitio dinámico entre el aparato 21 de impresora y la red 60 DMZ de impresora, como se muestra en la Figura 3c. El servidor 61 de impresión establece una conexión persistente al servidor 50a de aplicación, como se muestra en la Figura 3d. En la Figura 3e, una sucursal 15 bancaria emite una solicitud de emisión instantánea de tarjeta al servicio 20 web de sistema. El servicio web de sistema a continuación envía una solicitud HTTP POST a la red 55 DMZ de servicio web (servidor 56 de intermediario), como se muestra en la Figura 3f. El HTTP POST se envía al servidor 50a de aplicación y el estado de HTTP se devuelve al servicio 20 web, como se muestra en la Figura 3 g.

El servidor 50a de aplicación solicita un Criptograma de Clave de CW de tarjeta como es conocido en la técnica desde el servidor 50b de aplicación (Figura 3h). El servidor 50b de aplicación envía esta solicitud a la base de datos 40 de proveedor de servicios de tarjeta y devuelve los resultados al servidor 50a de aplicación (Figura 3i). El servidor 50a de aplicación entra en contacto con el HSM 47 mediante HTTP (9090), envía el Criptograma o Criptogramas de Clave de CW y datos de personalización de tarjeta, y recupera valores CV1 y CV2, de nuevo como es conocido en la técnica (Figura 3j).

El servidor 50a de aplicación entra en contacto con el servidor 50b de aplicación y solicita información de cálculo de imagen de tarjeta (Figura 3k). El servidor 50b de aplicación recupera la información de cálculo de imagen desde la base de datos 40 y devuelve los resultados (Figura 3l). El servidor 50a de aplicación conecta al servidor 50b de aplicación y solicita los datos de imagen de tarjeta (Figura 3m). El servidor 50b de aplicación recupera los datos de imagen de tarjeta desde el servidor 42 de ficheros y los transmite de vuelta a través de la solicitud de HTTP (Figura 3n).

Como se muestra en la Figura 3o, el servidor 50a de aplicación a continuación conecta al servidor 50b de aplicación para recuperar datos de cálculo de banda magnética de tarjeta. El servidor 50b de aplicación recupera los datos de cálculo de banda magnética desde la base de datos 40 y devuelve los resultados al servidor 50a de aplicación a través de la respuesta de HTTP (Figura 3p).

Teniendo ahora los valores de tarjeta CV1 y CV2, los datos de personalización de tarjeta, la información de imagen de tarjeta, los datos de imagen de tarjeta, y los datos de banda magnética, el servidor 50a de aplicación comunica el trabajo de impresión de tarjetas en un bus de mensaje (Figura 3q). El agente de conexión a continuación asigna el trabajo a un subproceso de trabajador en el servidor 61 de impresión (Figura 3r). El servidor 61 de impresión envía el trabajo de impresión a la impresora 18 a través del túnel de VPN de sitio a sitio dinámico (Figura 3s). La impresora 18 a continuación intenta imprimir la tarjeta y envía un mensaje de respuesta de impresión de tarjetas (éxito/fallo/intervención de usuario requerida) de vuelta al servidor 61 de impresión (Figura 3t). El subproceso de trabajador pone el resultado de impresión en el bus de mensaje (Figura 3u). El servidor 50a de aplicación envía el resultado de impresión a la red 55 DMZ de servicio web (servidor 56 de intermediario) mediante HTTP POST (Figura 3v). El servidor 56 de intermediario retransmite el resultado de impresión al servicio 20 web de sistema (Figura 3w) que retransmite el resultado a la sucursal 15 solicitante (Figura 3x), que completa el proceso. El sistema 10 ahora está listo para otra solicitud de impresión de tarjetas.

En el proceso anteriormente descrito, aunque muchas de las etapas de recuperación de datos se realizan secuencialmente, esto no se requiere. Por ejemplo, algunos o todos los datos necesarios de los servidores como se ilustra y describe con referencia a las Figuras 3h-3q pueden recuperarse de manera concurrente en una única etapa.

Por lo tanto, aunque se han descrito realizaciones particulares de la presente invención de un nuevo y útil sistema y método para emisión instantánea de tarjetas de transacción financiera personalizadas, no se pretende que tales referencias se interpreten como limitaciones al alcance de esta invención excepto como se expone en las siguientes reivindicaciones.

REIVINDICACIONES

1. Un sistema (10) para emisión instantánea de tarjetas de transacción financiera en respuesta a solicitudes de tarjeta realizadas por clientes en una o más localizaciones (15) de sucursal asociadas con una institución financiera, en el que las solicitudes de tarjeta cada una incluye información de cliente asociada con un cliente e información de tarjeta que incluye número de identificación personal, PIN, información de tarjeta a asociarse con una tarjeta de transacción financiera, comprendiendo el sistema:

redes (35, 35a, y 35b) de proveedor de servicios de tarjetas;
al menos un terminal (16) de datos de sucursal en cada localización (15) de sucursal, en el que el terminal (16) de datos de sucursal es eficaz para recibir la información de cliente y al menos la información de tarjeta de PIN asociada con una solicitud de tarjeta, está funcionalmente acoplado mediante una conexión de comunicaciones de datos seguras a las redes (35, 35a y 35b) de proveedor de servicio de tarjeta, y es eficaz para transmitir la solicitud de tarjeta con la información de cliente y al menos la información de tarjeta de PIN a las redes (35, 35a y 35b) de proveedor de servicios de tarjeta mediante la conexión de comunicaciones de datos seguras, mientras los clientes están presentes en la una o más localizaciones (15) de sucursal;
en el que las redes (35, 35a y 35b) de proveedor de servicios de tarjeta comprenden:

una red (36, 36a) de servidor de emisión instantánea que incluye un servidor (50a) de aplicación;
una red (45) de personalización de tarjeta de emisión instantánea acoplada a la red (36, 36a) de servidor de emisión instantánea y que incluye un módulo de seguridad de anfitrión de hardware (HSM) (47) para proporcionar funciones criptográficas para encriptación de datos de tarjeta;
una red (60) perimetral de impresión de emisión instantánea acoplada a la red (36, 36a) de servidor de emisión instantánea y que incluye un servidor (61) de impresión que aloja el software de aplicación de impresión de tarjetas;
un servidor (41) de base de datos conectado a una base de datos (40) de PIN que almacena de manera segura la información de tarjeta de PIN asociada asociada con cada solicitud de tarjeta;
en el que en respuesta a una solicitud de tarjeta el servidor (50, 50a) de aplicación es operable para comunicar cada trabajo de impresión de tarjetas que incluye un fichero de tarjeta asociado al servidor (61) de impresión; y,

una red (17) de impresora de tarjetas de sucursal aislada en cada localización (15) de sucursal y que incluye una impresora (18) de tarjetas asociada, en la que cada red (17) de sucursal está funcionalmente acoplada mediante otra conexión de comunicaciones de datos seguras a la red (60) perimetral de impresión de emisión instantánea, y en el que el servidor (61) de impresión es operable para transmitir de manera segura cada trabajo de impresión de tarjetas con comandos de impresión a una impresora (18) de tarjetas asociada que es operable para imprimir una tarjeta de transacción financiera personalizada, en respuesta a recibir de manera segura el trabajo de impresión de tarjetas con comandos de impresión transmitidos por el servidor (61) de impresora de tarjetas de la red (60) perimetral de impresión de emisión instantánea de las redes (35, 35a y 35b) de proveedor de servicio de tarjeta, mientras que los clientes están presentes en la una o más localizaciones (15) de sucursal.

2. El sistema (10) de la reivindicación 1, en el que las redes (35, 35a y 35b) de proveedor de servicios de tarjeta incluyen una red (55) perimetral de servicio web instantáneo para proporcionar una interfaz entre el enlace de comunicaciones de datos seguro y la red (36, 36a) de servidor de emisión instantánea, y que comprende adicionalmente:

un servicio (20) web de sistema acoplado a los terminales (16) de datos de sucursal en el que los terminales (16) de datos de sucursal comunican de manera segura con las redes (35, 35a) de proveedor de servicios de tarjeta a través del servicio (20) web de sistema, en el que el sistema (10) es operativo para proporcionar funcionalidad de túnel de red privada virtual (VPN) acoplado al servicio (20) web de sistema, y a las redes (35, 35a y 35b) de proveedor de servicios de tarjeta a través de una red (5) pública, y en el que tal túnel de VPN es eficaz para proporcionar comunicaciones encriptadas entre el servicio (20) web de sistema y la red (55) perimetral de servicio web instantáneo usando un primer aparato (59) de seguridad.

3. El sistema (10) de la reivindicación 2, en el que la red (55) perimetral de servicio web instantáneo incluye un servicio (56) web de proveedor de servicios de tarjeta, y en el que el servicio (56) web de proveedor de servicios de tarjeta y el servicio (20) web de sistema son operables para generar una o más interfaces de usuario para visualizar en cada terminal (16) de datos de sucursal para su uso al solicitar una tarjeta de transacción financiera.

4. El sistema (10) de una cualquiera de las reivindicaciones 1-3, en el que el sistema (10) es operativo para proporcionar una funcionalidad de túnel de red privada virtual, VPN, acoplado a la red (60) perimetral de impresión de emisión instantánea y a la red (17) de impresora de tarjetas de sucursal en cada localización (15) de sucursal a través de una red (5) pública, en el que la red (17) de impresora de tarjetas de sucursal en cada localización (15) de sucursal comprende adicionalmente otra funcionalidad de aparato (19, 21) de seguridad acoplado a la impresora (18) de tarjetas asociada, y en el que tal túnel de VPN es eficaz para proporcionar comunicaciones encriptadas entre la red (60)

perimetral de impresión de emisión y la red (17) de impresora de tarjeta de sucursal asociada en cada localización (15) de sucursal usando el otro aparato (19, 21) de seguridad y un segundo aparato (62) de seguridad.

5. El sistema (10) de la reivindicación 4, en el que el otro aparato (21) de seguridad de la red (17) de impresora de tarjetas de sucursal en cada localización (15) de sucursal es operativo como un punto terminal dinámico para iniciar y mantener el túnel de VPN asociado que está funcionalmente acoplado a la red (60) perimetral de impresión de emisión instantánea usando el segundo aparato (62) de seguridad como un punto terminal estático.

6. El sistema (10) de una cualquiera de las reivindicaciones 1-5 en el que la impresora (18) de tarjetas de sucursal de la red (17) de impresora de tarjetas de sucursal en cada localización (15) de sucursal es eficaz para comunicar mensajes de éxito o fallo de trabajo de impresión de tarjetas al servidor (61) de impresora de la red (60) perimetral de impresión de emisión instantánea, y el servidor (61) de impresión es eficaz para comunicar mensajes de éxito o fallo de trabajo de impresión de tarjetas al servidor (50, 50a) de aplicación de la red (36, 36a) de servidor de emisión instantánea.

7. El sistema (10) de la reivindicación 6, en el que en respuesta a la comunicación de mensajes de éxito o fallo de trabajo de impresión de tarjetas por el servidor (61) de impresión al servidor (50, 50a) de aplicación, el servidor (50, 50a) de aplicación es eficaz para comunicar información de éxito o fallo de impresión de tarjetas a un terminal (16) de sucursal bancaria en la localización (17) de la sucursal desde la que se comunicó un correspondiente mensaje de éxito o fallo de trabajo de impresión de tarjetas al servidor (61) de impresión.

8. El sistema (10) de una cualquiera de las reivindicaciones 1-7, en el que cada trabajo de impresión de tarjetas y fichero de tarjeta incluido transmitido por el servidor (61) de impresora de tarjetas a una impresora (18) de tarjetas asociada incluye datos de personalización de tarjeta y datos de imagen de tarjeta.

9. El sistema (10) de la reivindicación 1, en el que en respuesta a una solicitud de tarjeta recibida en el servidor (50a) de aplicación software asociado con la base de datos (40) genera un número de referencia que se almacena en un fichero de datos de tarjeta asociado, y en el que el número de referencia se usa por el módulo (47) de seguridad de hardware-anfitrión para recuperar la información de la tarjeta de PIN asociada para su uso al aplicar cálculos al fichero de datos de tarjeta asociado.

10. El sistema (10) de la reivindicación 1 o la reivindicación 8, en el que las redes (35a y 35b) de proveedor de servicios de tarjeta comprenden adicionalmente:

otra red (36b) de servidor de emisión instantánea que incluye otro servidor (50b) de aplicación para recuperar datos de tarjeta de la base de datos (40) que se solicita por servidor (50a) de aplicación.

11. El sistema (10) de una cualquiera de las reivindicaciones 1-10, en el que la red (36, 36a) de servidor de emisión instantánea está acoplada a la red (55) de impresora de servicio web a través de un tercer aparato (58) de seguridad, en el que la red (60) perimetral de impresión de emisión instantánea está conectada a la red (36, 36a) de servidor de emisión instantánea a través de un cuarto aparato (38) de seguridad, y en el que el servidor (61) de impresión establece una conexión persistente al servidor (50, 50a) de aplicación.

12. El sistema (10) de la reivindicación 11, en el que dicha otra red (36b) de servidor de emisión está acoplada a la red (35a) de servidor de emisión instantánea a través del primer aparato (59) de seguridad, a la red (55) perimetral de servicio web instantáneo y al tercer aparato (58) de seguridad.

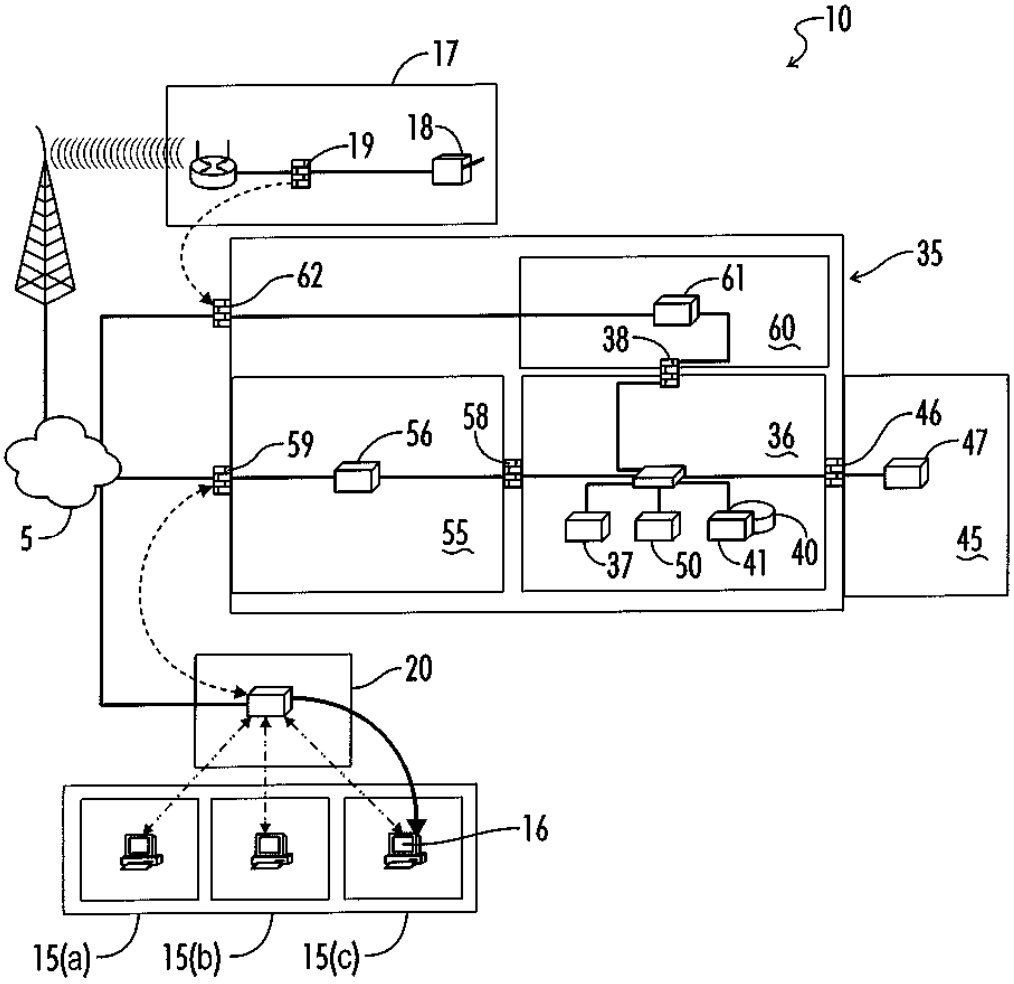
10
17
18
19
35
62
61
60
38
46
47
58
59
56
36
5
55
37
50
41
40
45
20
16
15(a)
15(b)
15(c)

FIG. 1(a)

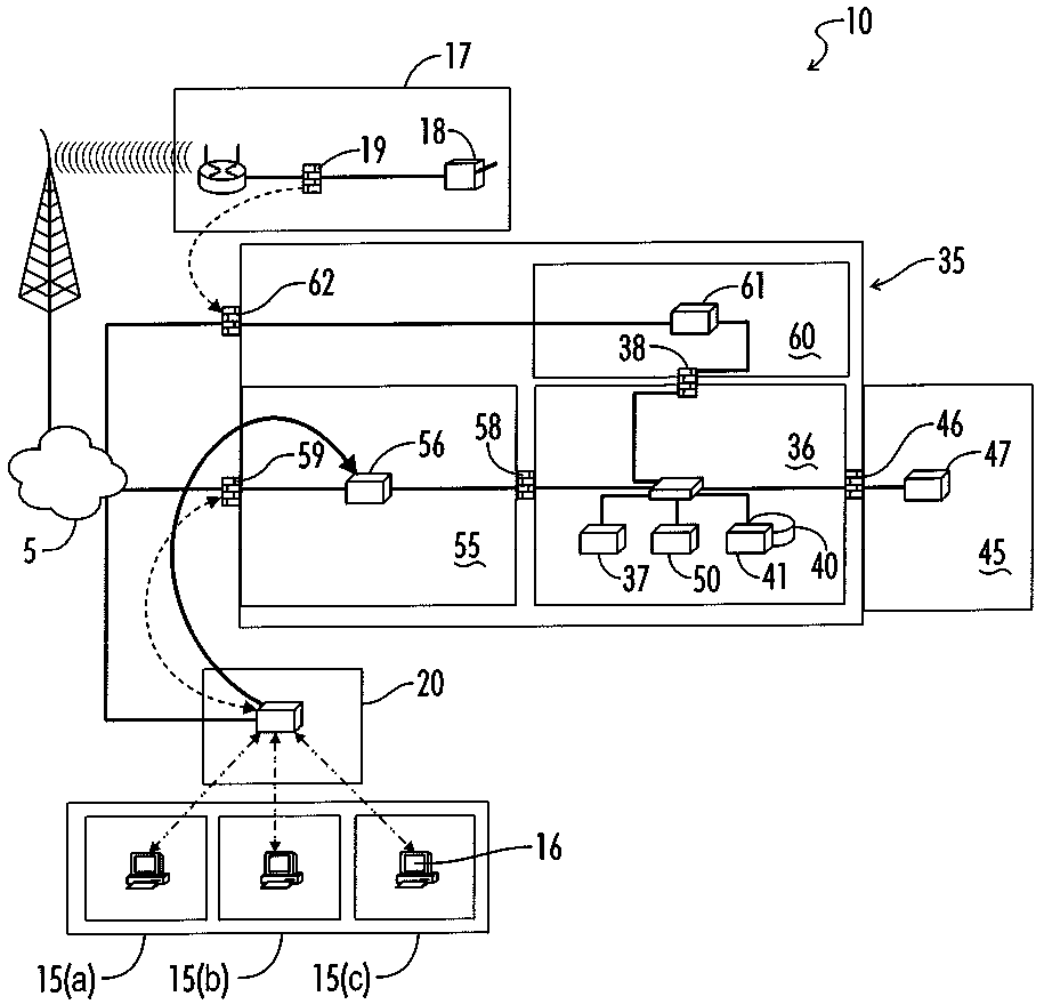
10
17
19
18
35
62
61
60
38
59
56
58
36
46
47
5
55
37
50
41
40
45
20
16
15(a)
15(b)
15(c)

FIG. 1(b)

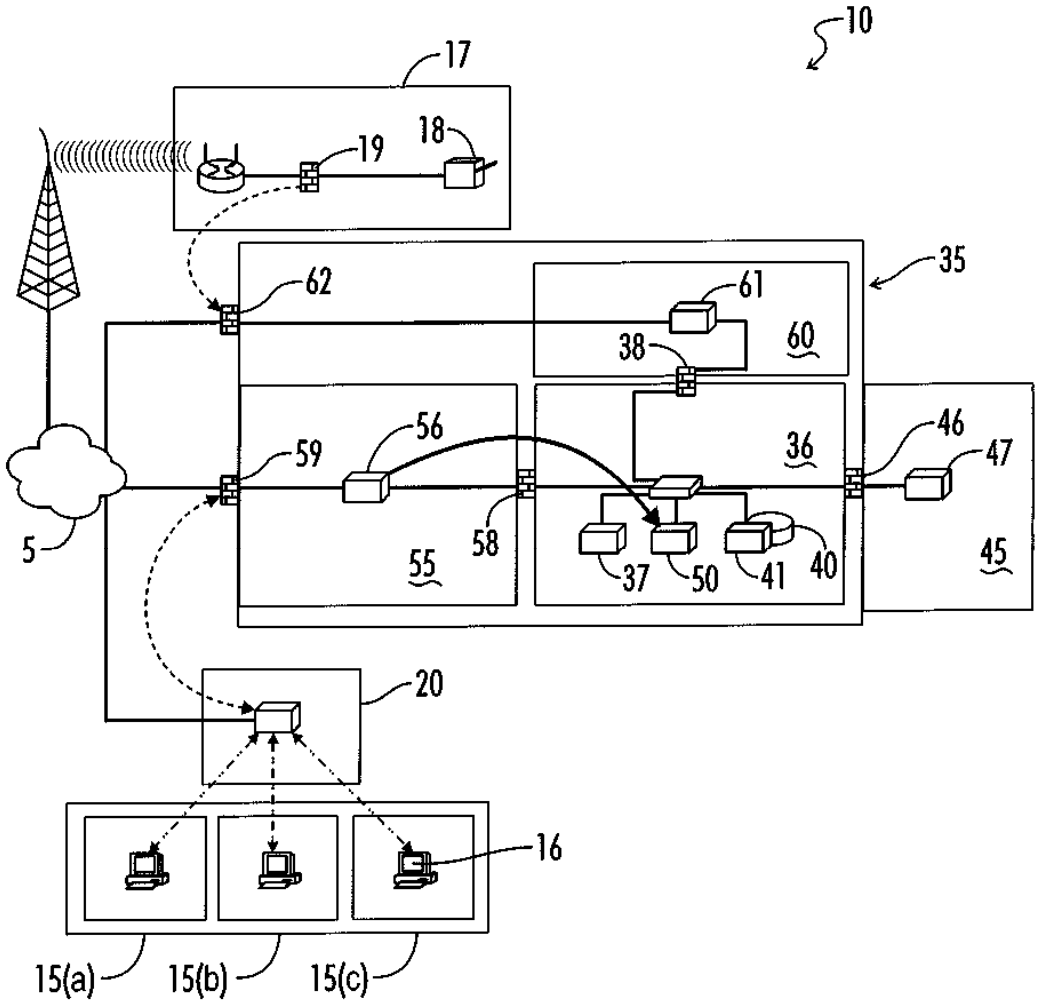
10
17
18
19
35
62
61
60
38
56
59
36
46
47
5
58
55
37
50
41
40
45
20
16
15(a)
15(b)
15(c)

FIG. 1(c)

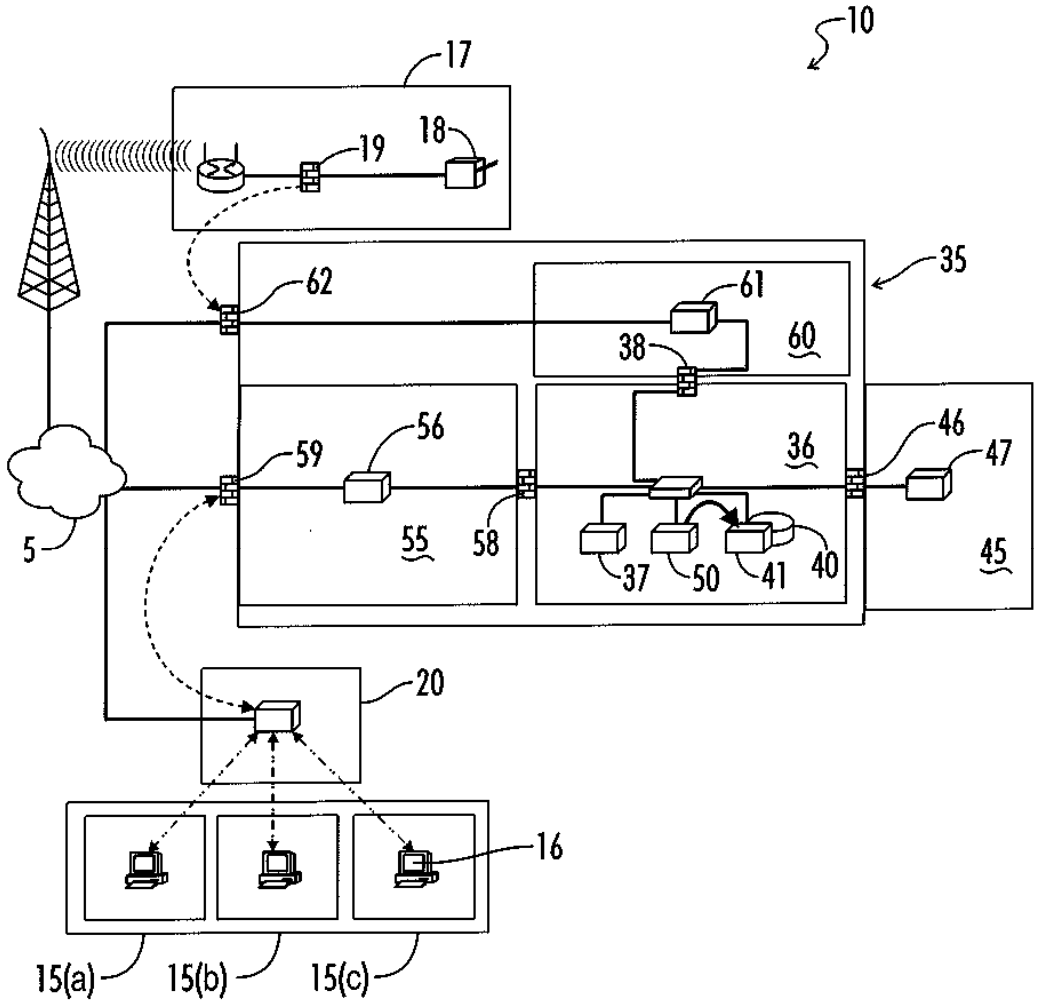
10
17
18
19
35
62
61
60
38
56
59
36
46
47
5
55
58
37
50
41
40
45
20
16
15(a)
15(b)
15(c)

FIG. 1(d)

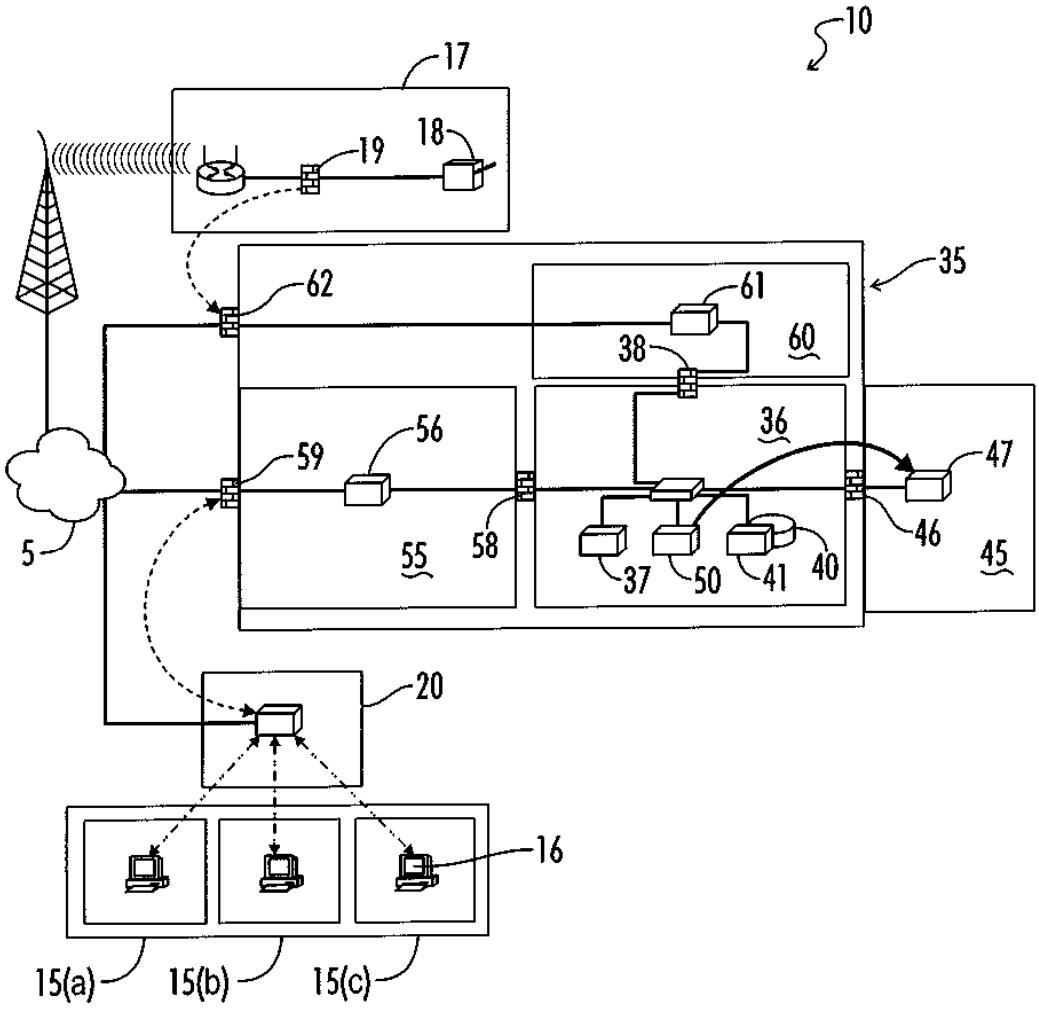
10
17
19
18
62
61
35
38
60
36
59
56
47
5
55
58
46
45
37
50
41
40
20
16
15(a)
15(b)
15(c)

FIG. 1(e)

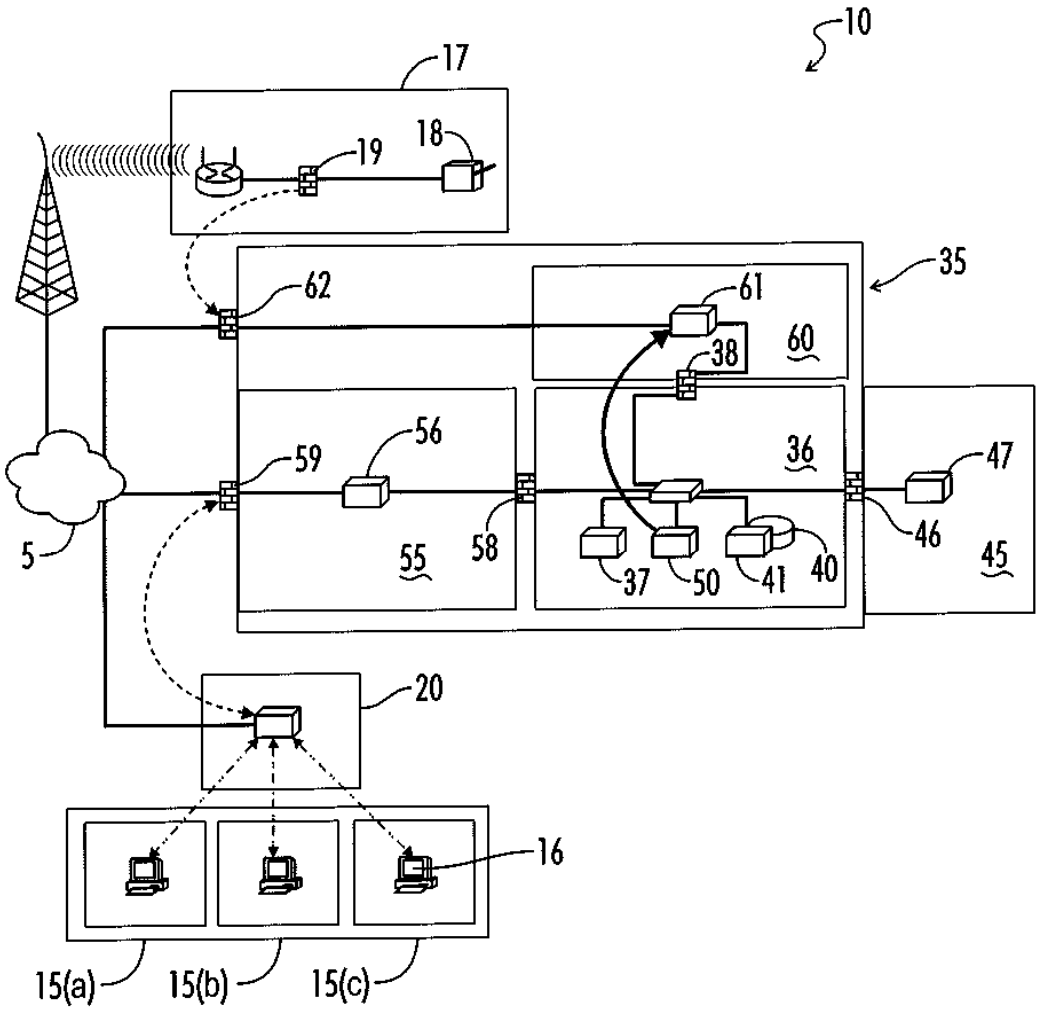
10
17
19
18
35
62
61
60
38
56
59
36
47
5
55
58
46
45
37
50
41
40
20
16
15(a)
15(b)
15(c)

FIG. 1(f)

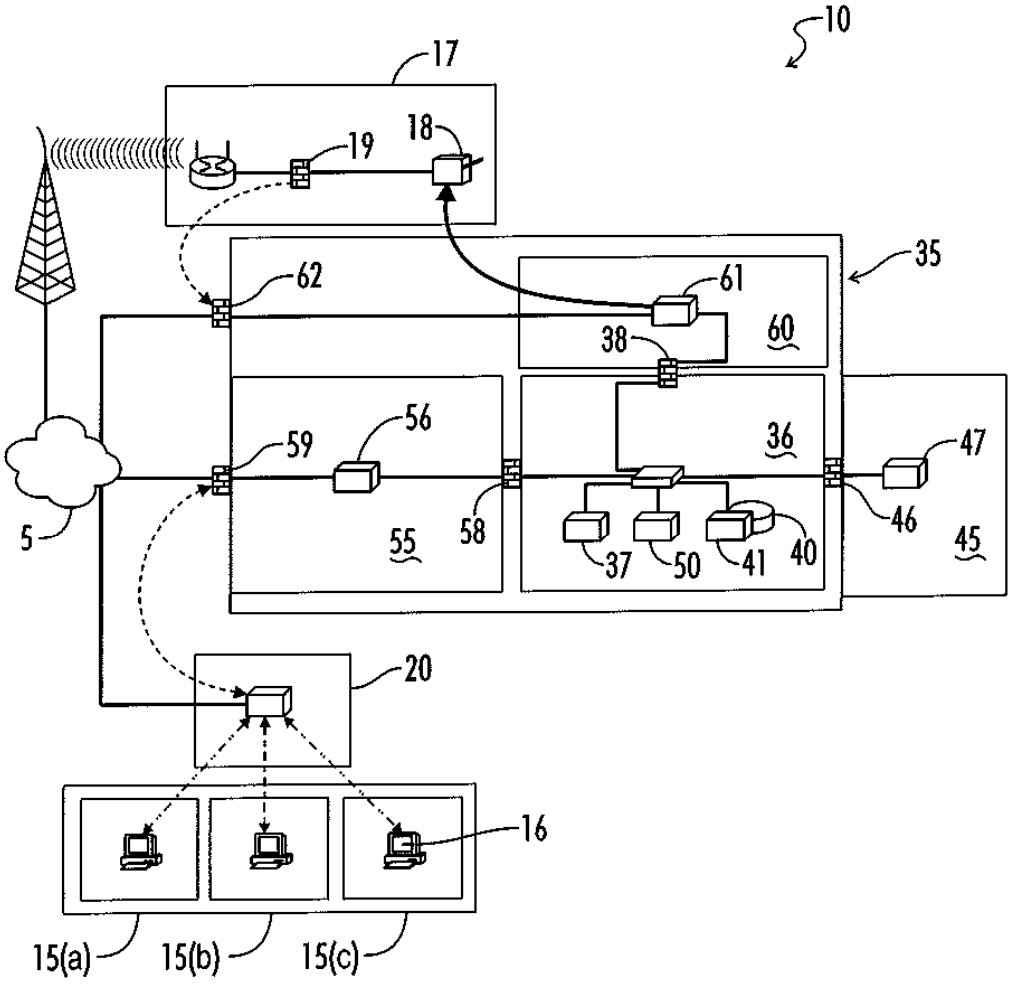
10
17
18
19
35
62
61
60
38
56
59
36
47
5
55
58
46
45
37
50
41
40
20
16
15(a)
15(b)
15(c)

FIG. 1(g)

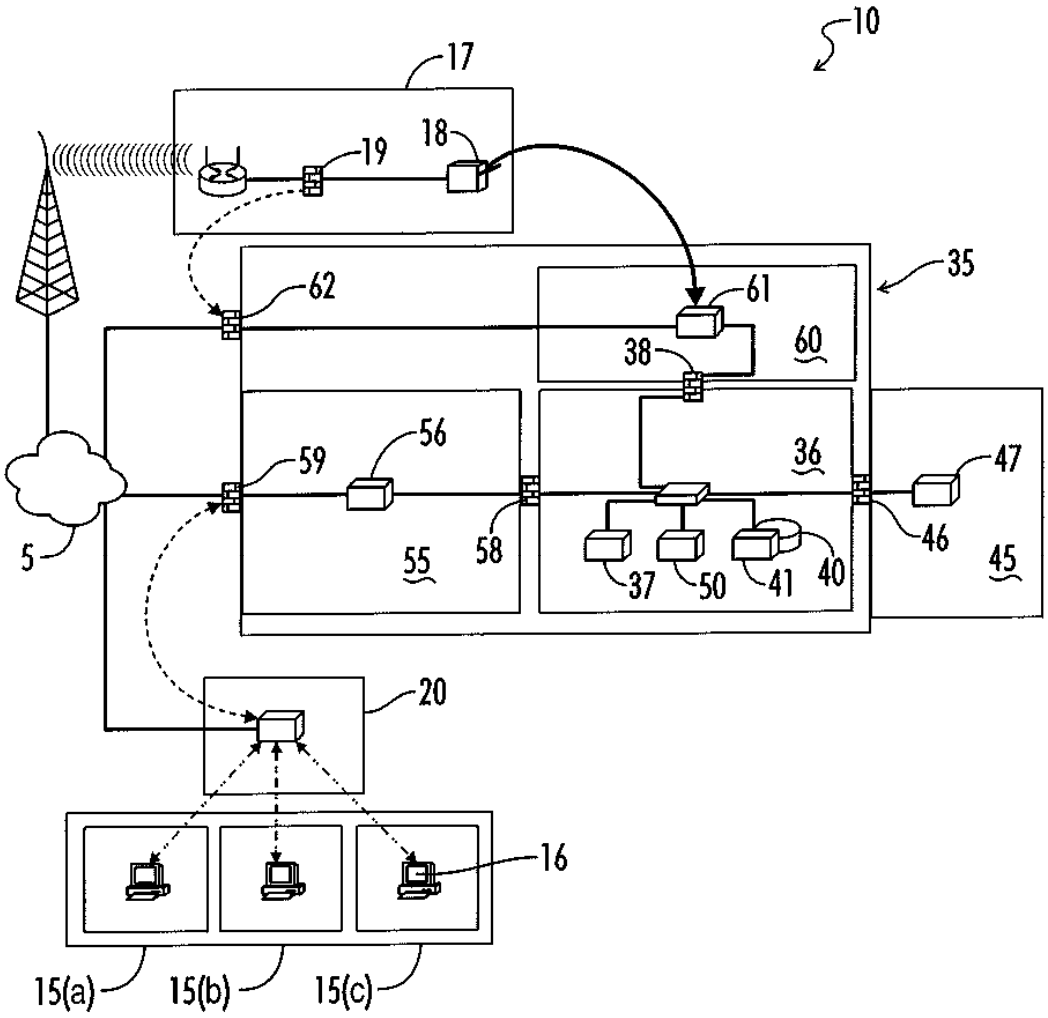
10
17
19
18
35
62
61
60
38
59
56
36
47
5
55
58
37
50
41
40
46
45
20
16
15(a)
15(b)
15(c)

FIG. 1(h)

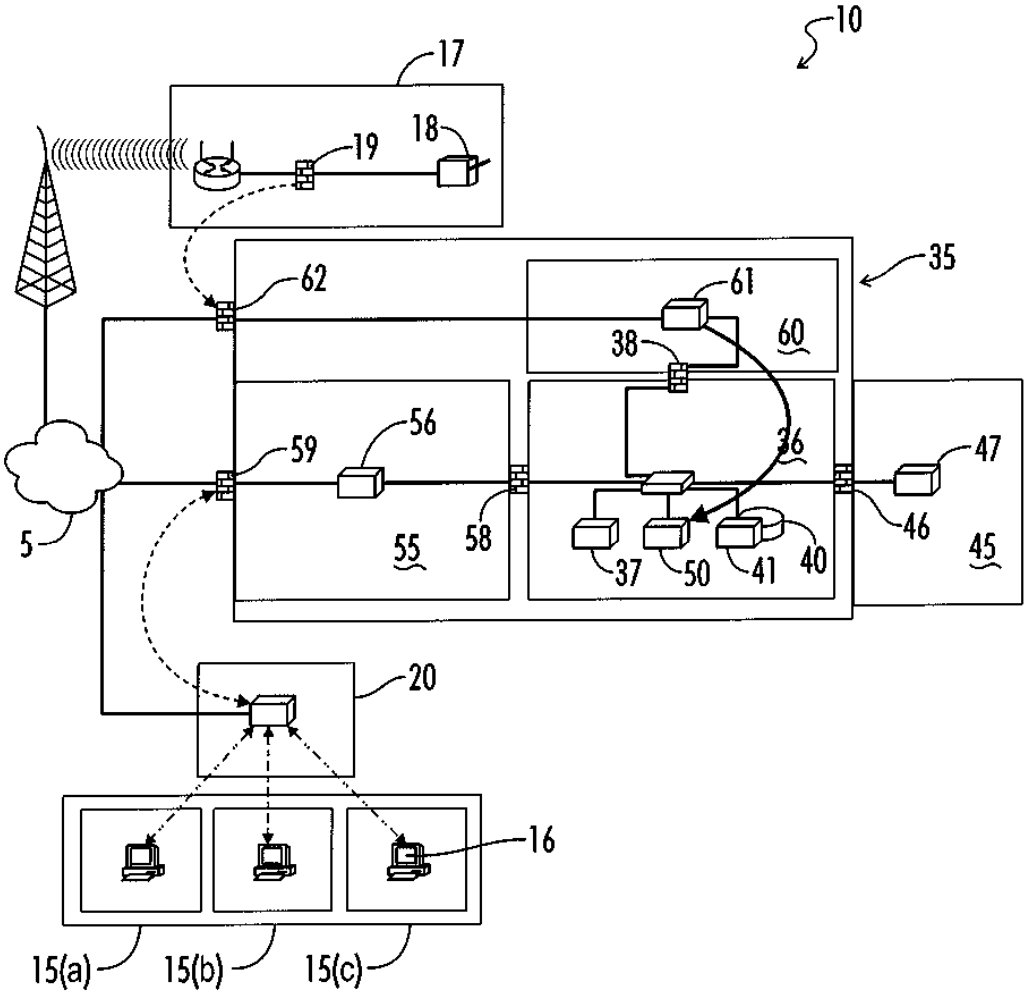
10
17
19
18
35
62
61
60
38
59
56
36
47
5
55
58
37
50
41
40
46
45
20
16
15(a)
15(b)
15(c)

FIG. 1(i)

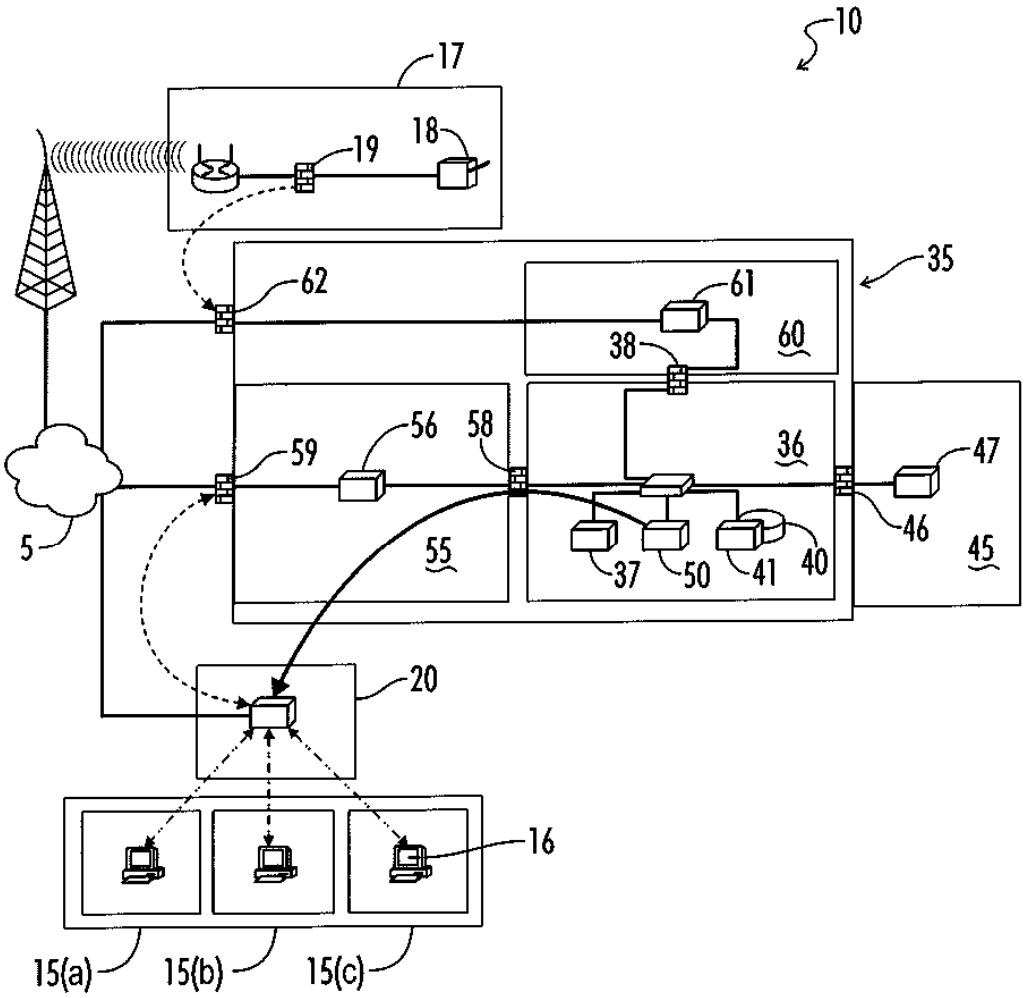
10
17
18
19
35
62
61
60
38
59
56
58
36
47
5
55
37
50
41
40
46
45
20
16
15(a)
15(b)
15(c)

FIG. 1(j)

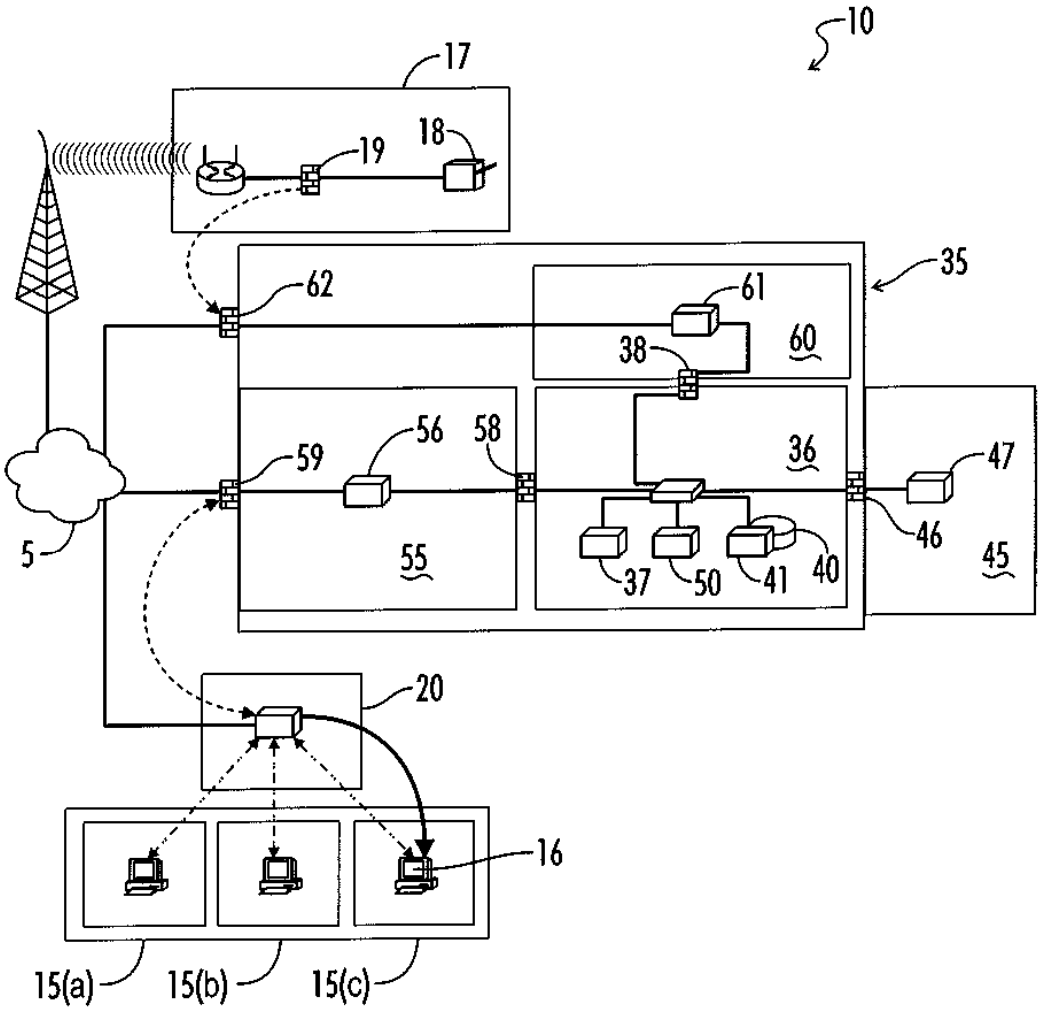
10
17
18
19
62
61
35
60
38
56
58
59
36
47
5
55
46
45
37
50
41
40
20
16
15(a)
15(b)
15(c)

FIG. 1(k)

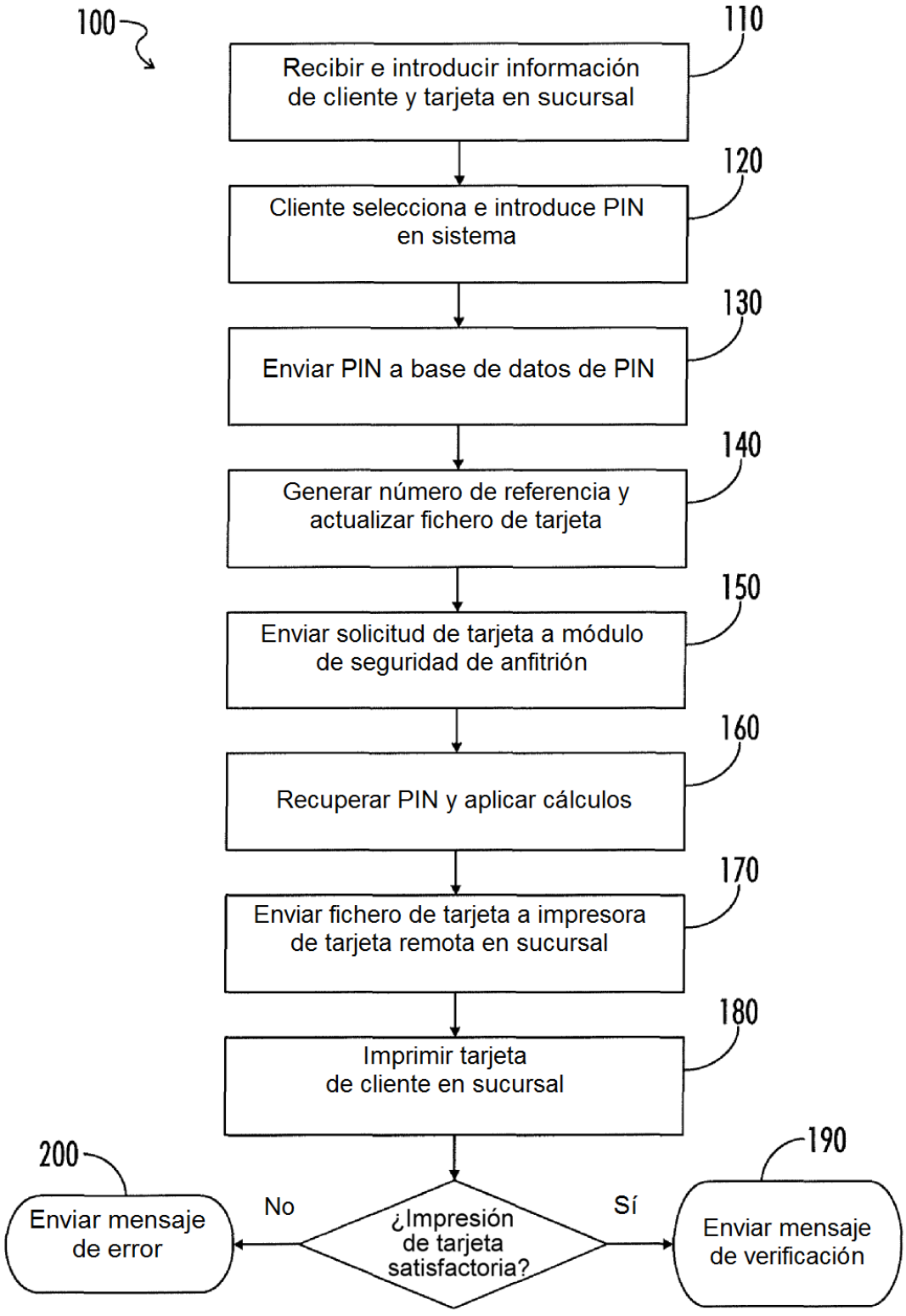
100
110
Recibir e introducir información de cliente y tarjeta en sucursal
120
Cliente selecciona e introduce PIN en sistema
130
Enviar PIN a base de datos de PIN
140
Generar número de referencia y actualizar fichero de tarjeta
150
Enviar solicitud de tarjeta a módulo de seguridad de anfitrión
160
Recuperar PIN y aplicar cálculos
170
Enviar fichero de tarjeta a impresora de tarjeta remota en sucursal
180
Imprimir tarjeta de cliente en sucursal
200
Enviar mensaje de error
No
¿Impresión de tarjeta satisfactoria?
Sí
190
Enviar mensaje de verificación

FIG. 2

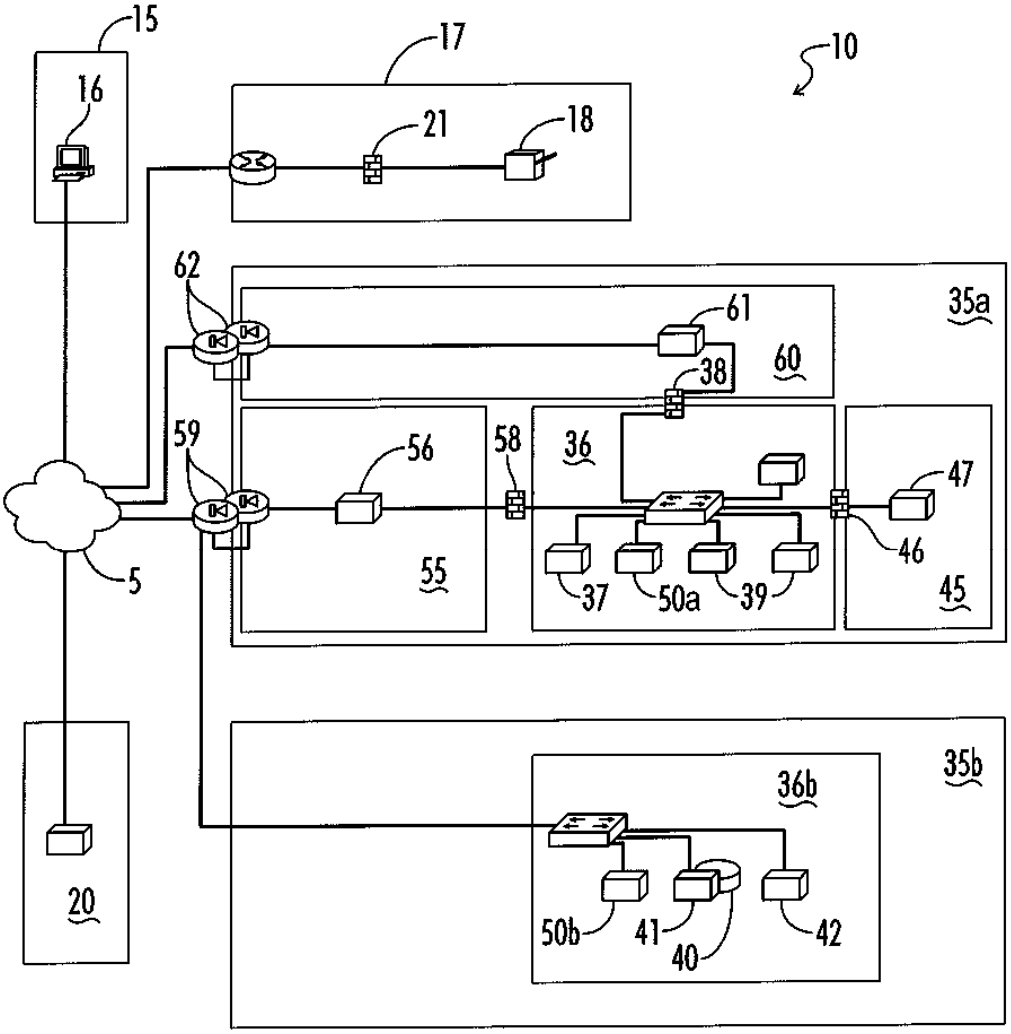
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
55
46
45
5
37
50a
39
35b
36b
20
50b
41
40
42

FIG. 3a

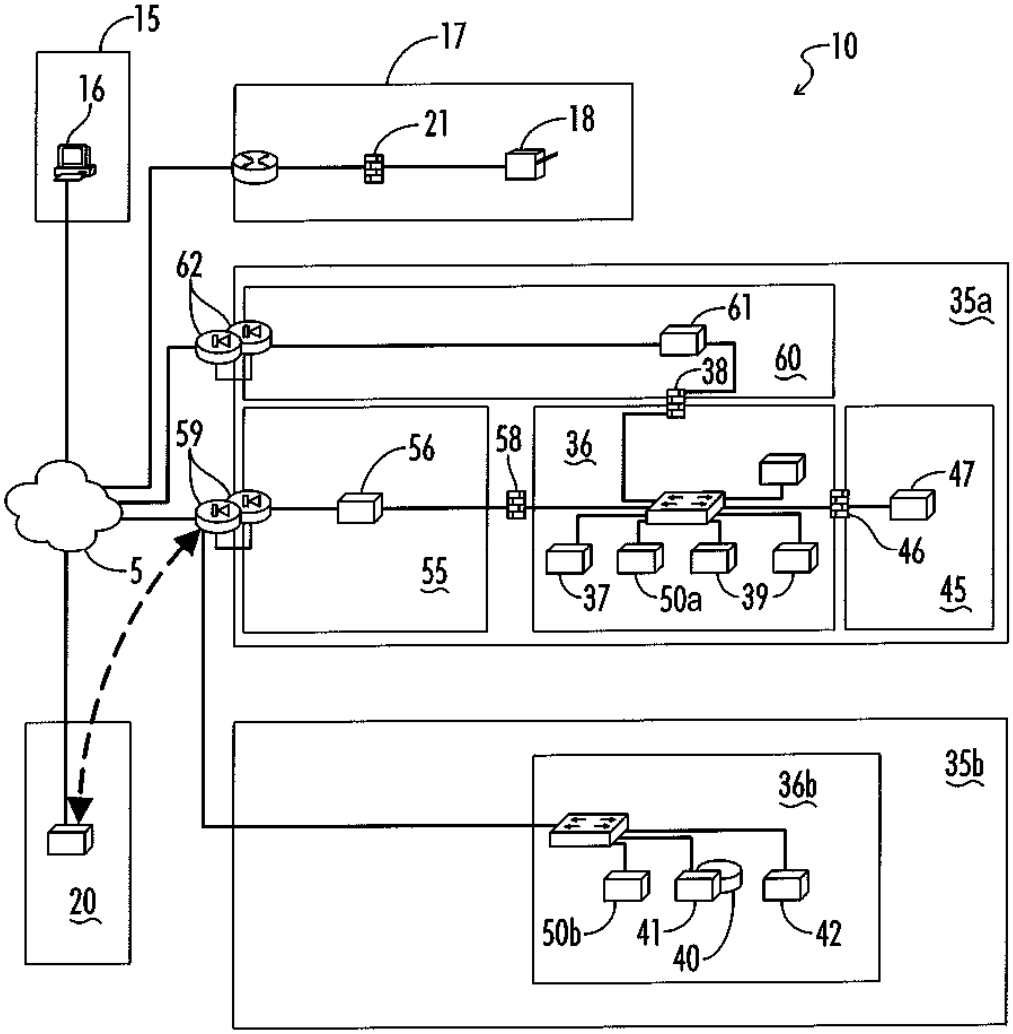
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
55
46
45
5
37
50a
39
35b
36b
20
50b
41
42
40

FIG. 3b

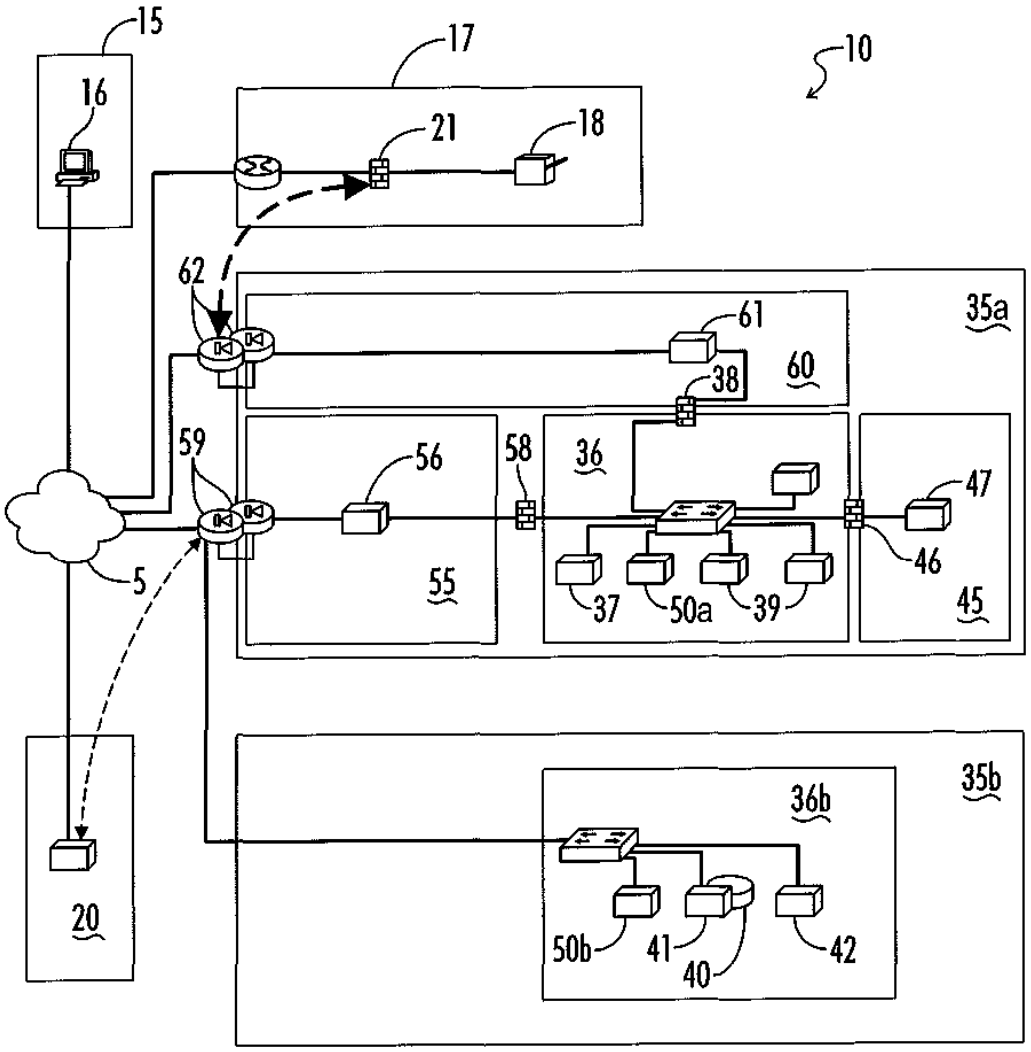
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
55
46
5
37
50a
39
45
35b
36b
20
50b
41
42
40

FIG. 3c

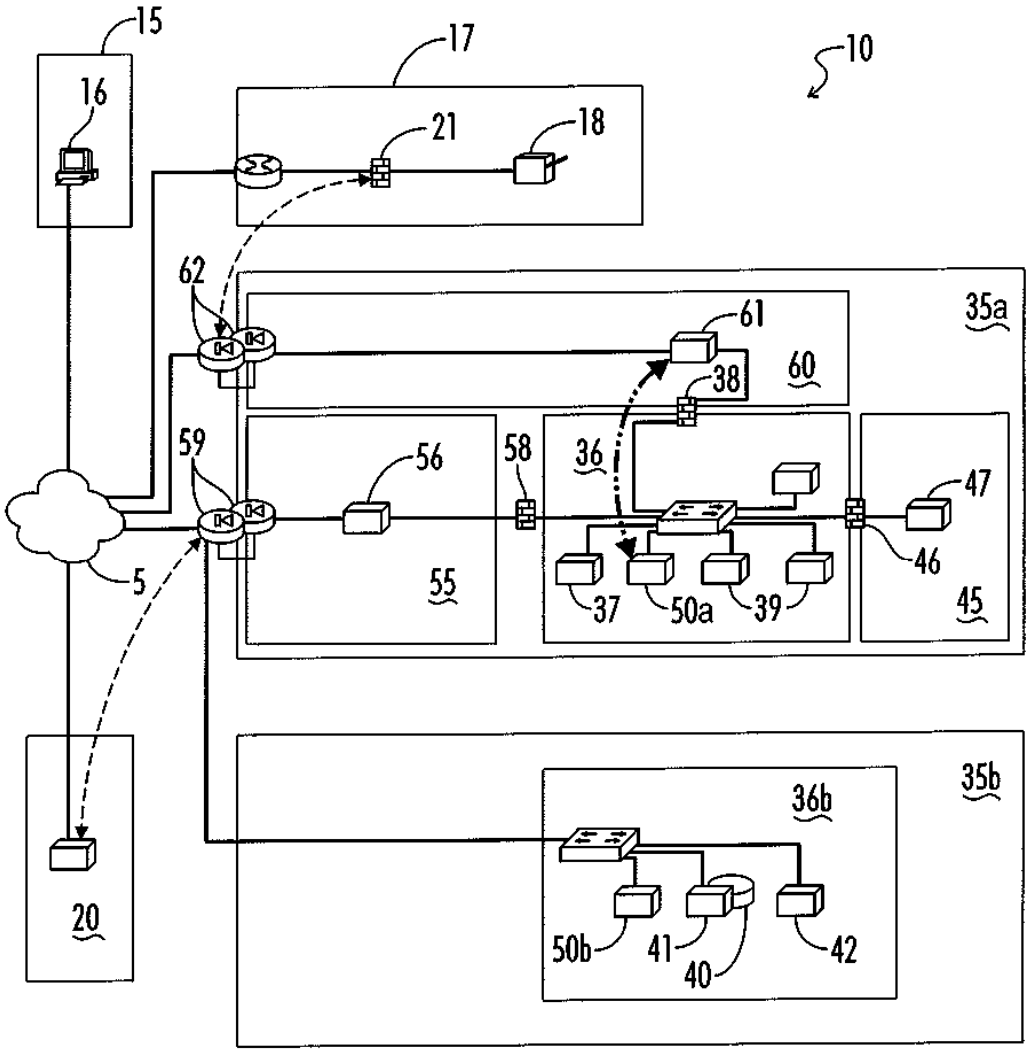
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
55
46
5
37
50a
39
45
35b
36b
20
50b
41
42
40

FIG. 3d

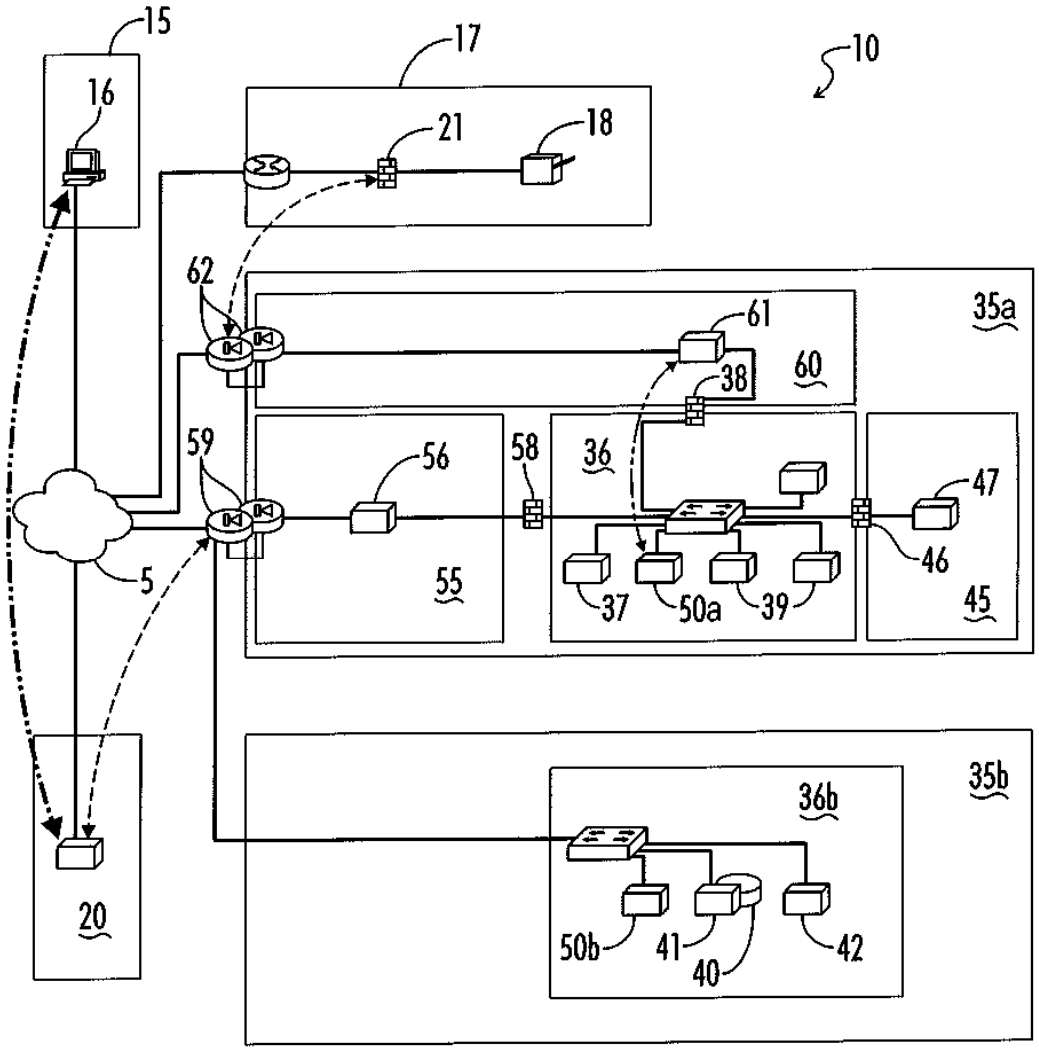
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
5
55
37
50a
39
46
45
35b
36b
20
50b
41
42
40

FIG. 3e

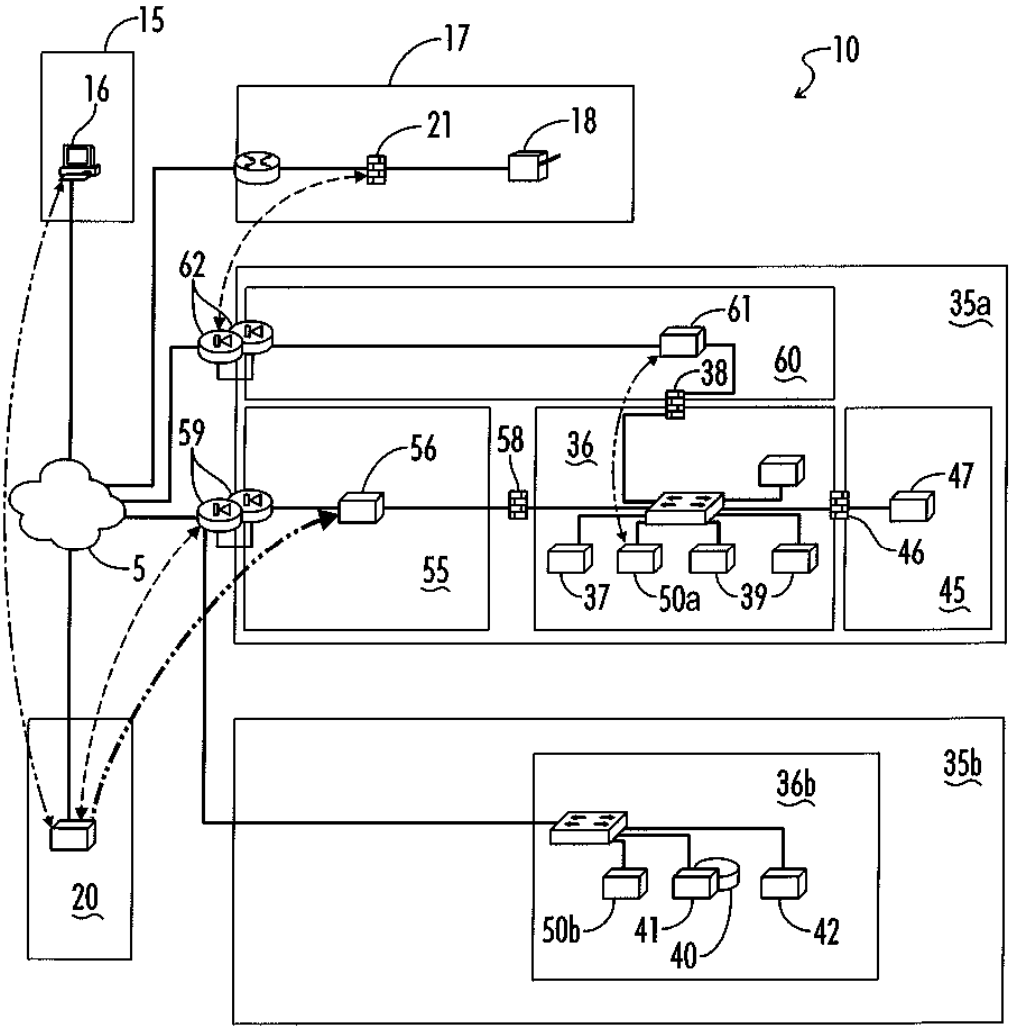
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
5
55
37
50a
39
46
45
35b
36b
20
50b
41
42
40

FIG. 3f

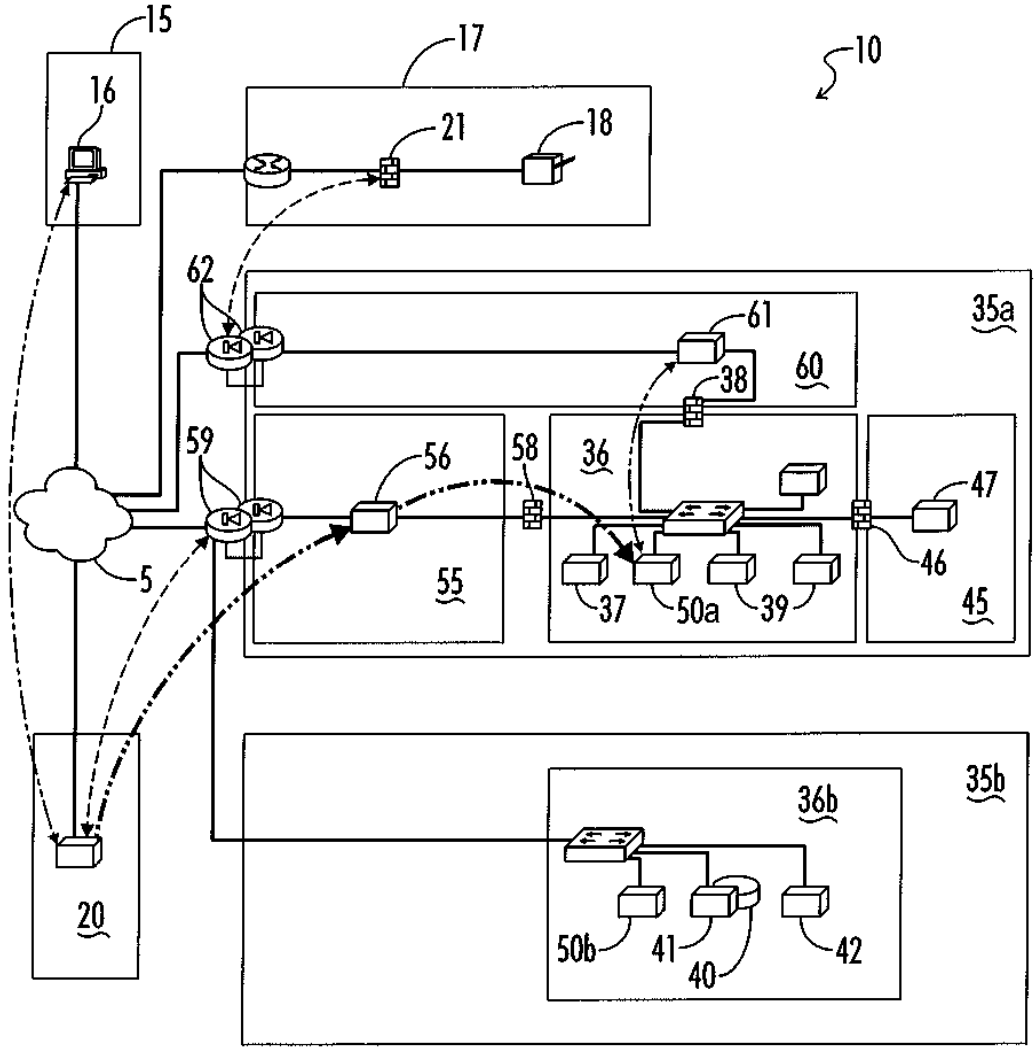
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
5
55
37
50a
39
46
45
35b
36b
20
50b
41
42
40

FIG. 3g

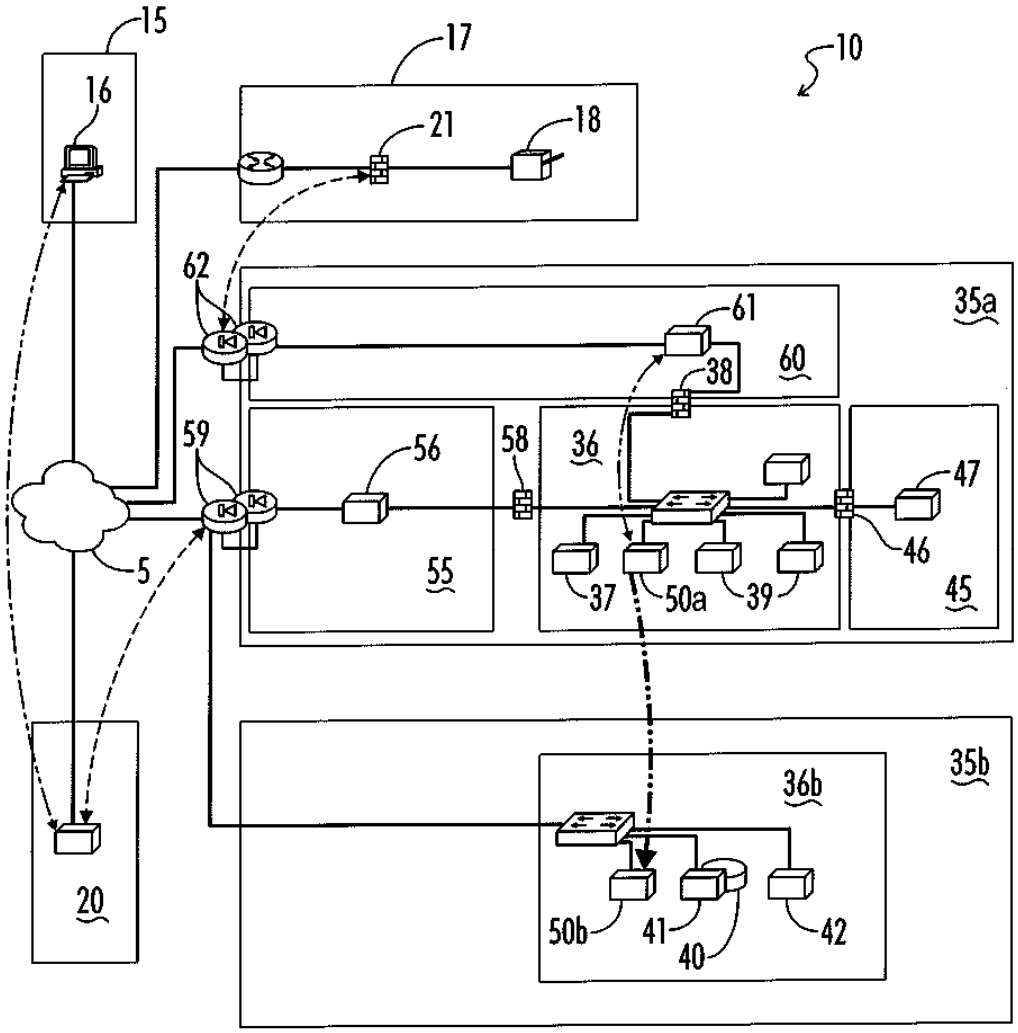
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
55
46
45
5
37
50a
39
35b
36b
20
50b
41
42
40

FIG. 3h

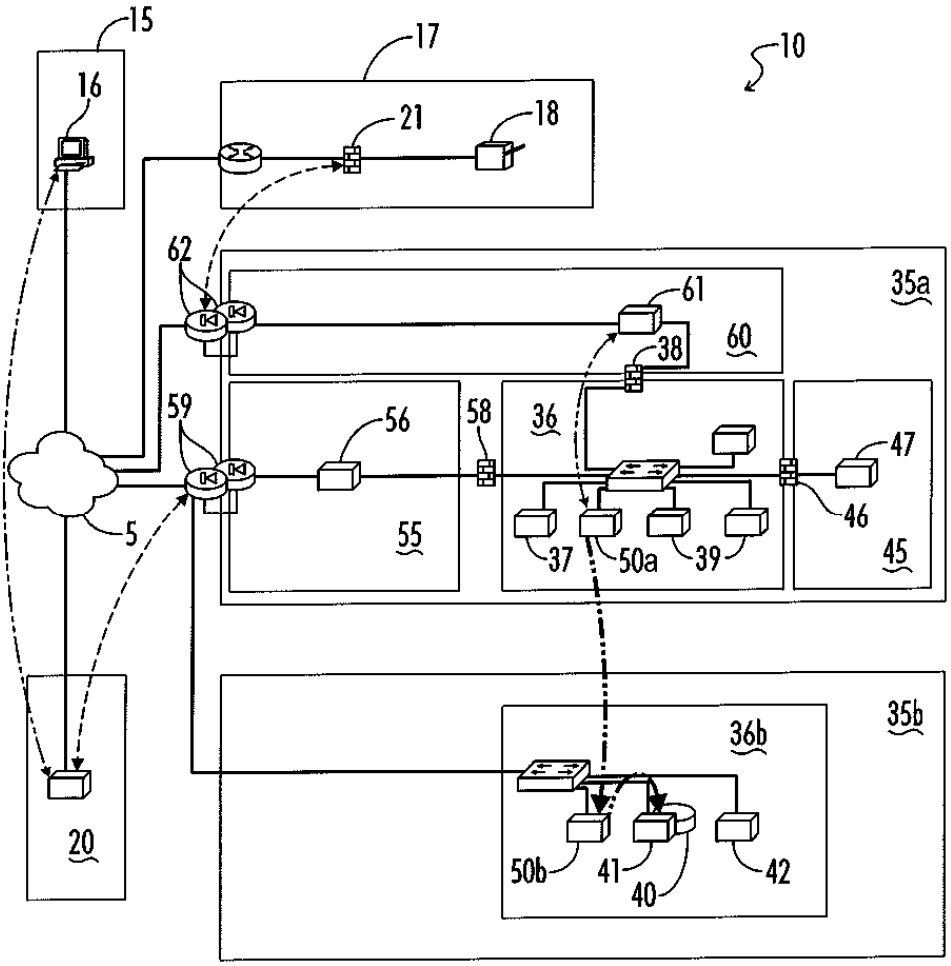
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
5
55
37
50a
39
46
45
35b
36b
20
50b
41
40
42

FIG. 3i

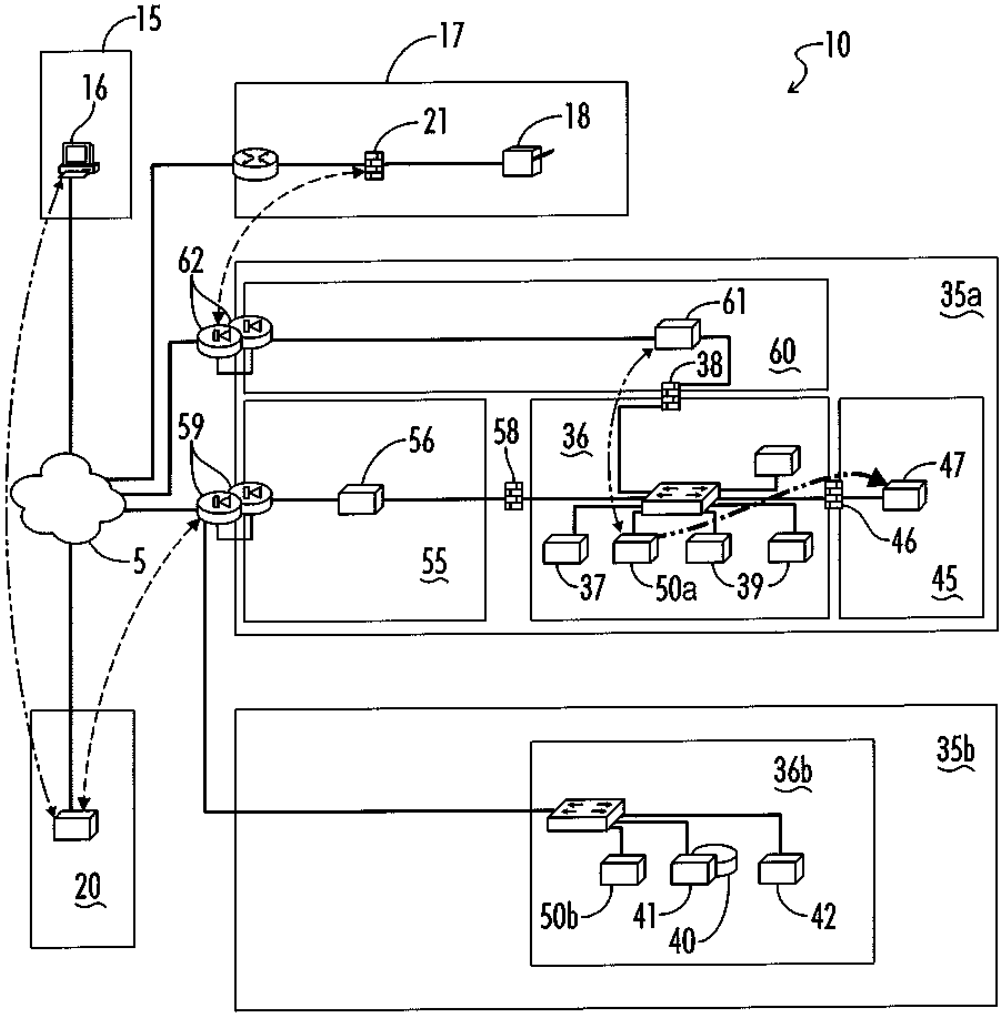
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
5
55
37
50a
39
46
45
35b
36b
20
50b
41
40
42

FIG. 3j

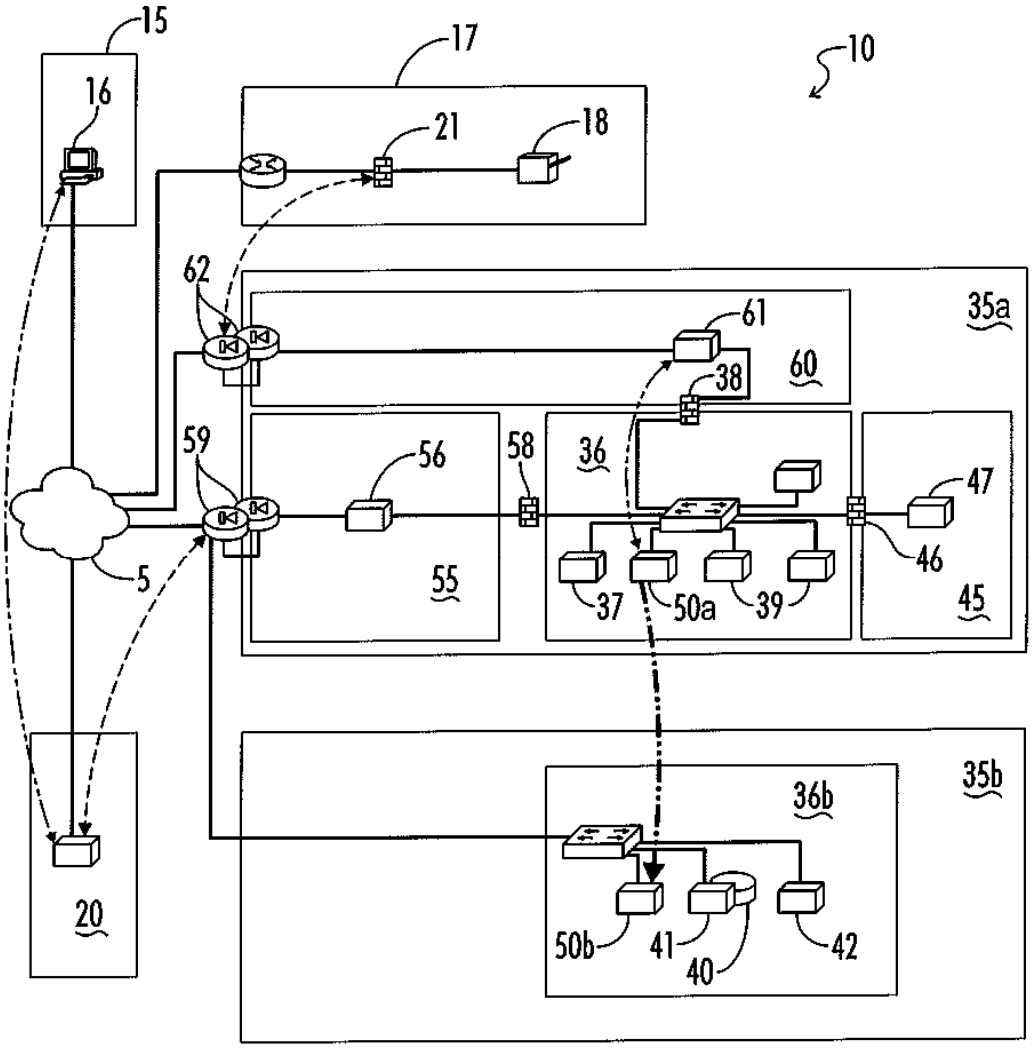
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
55
46
45
5
37
50a
39
35b
36b
20
50b
41
42
40

FIG. 3k

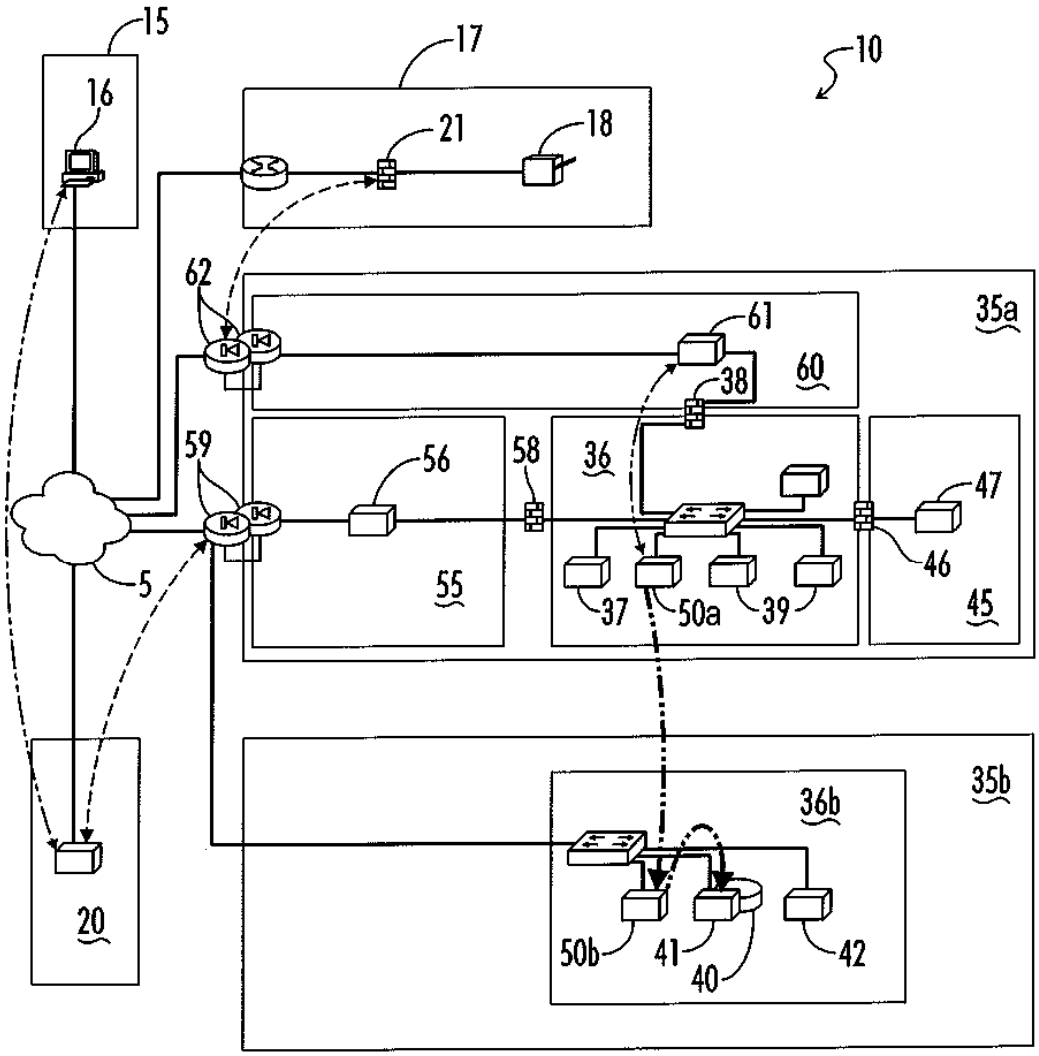
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
55
46
5
37
50a
39
45
35b
36b
20
50b
41
42
40

FIG. 31

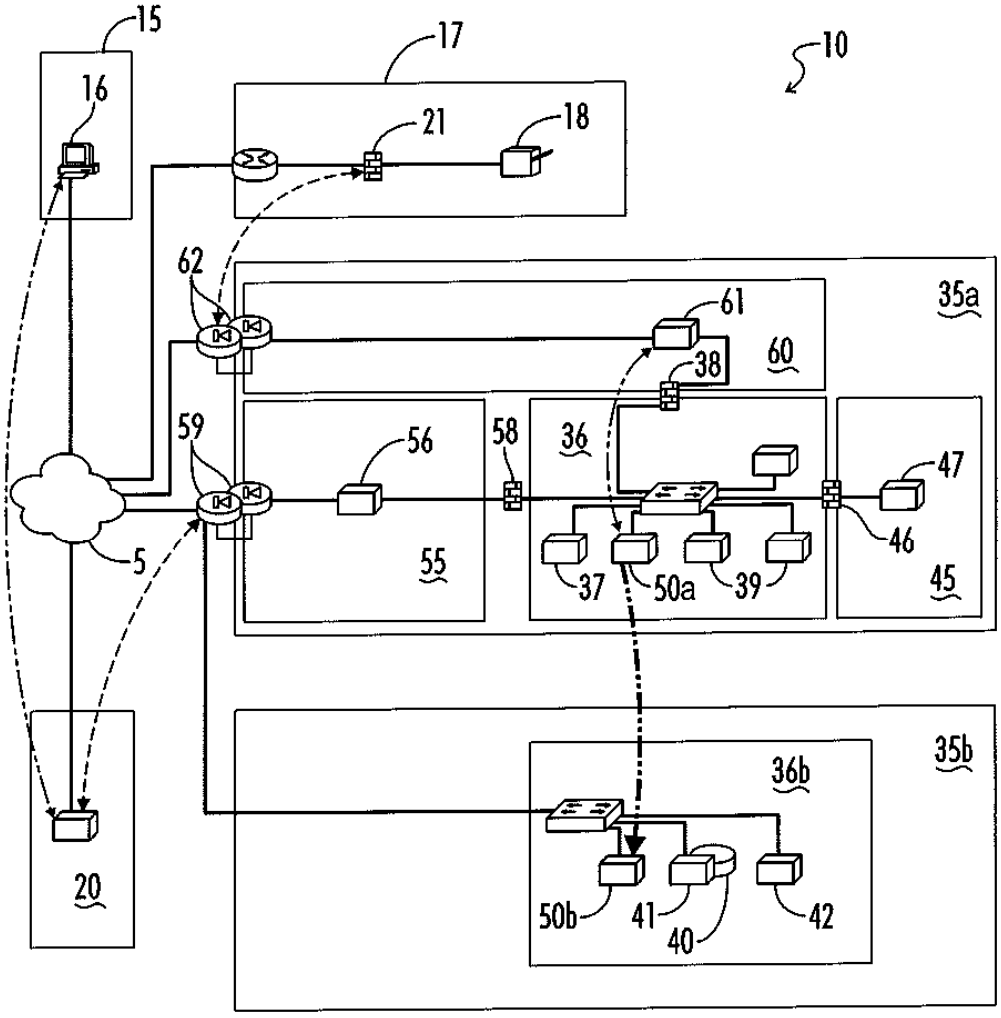
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
5
55
37
50a
39
46
45
35b
36b
20
50b
41
40
42

FIG. 3m

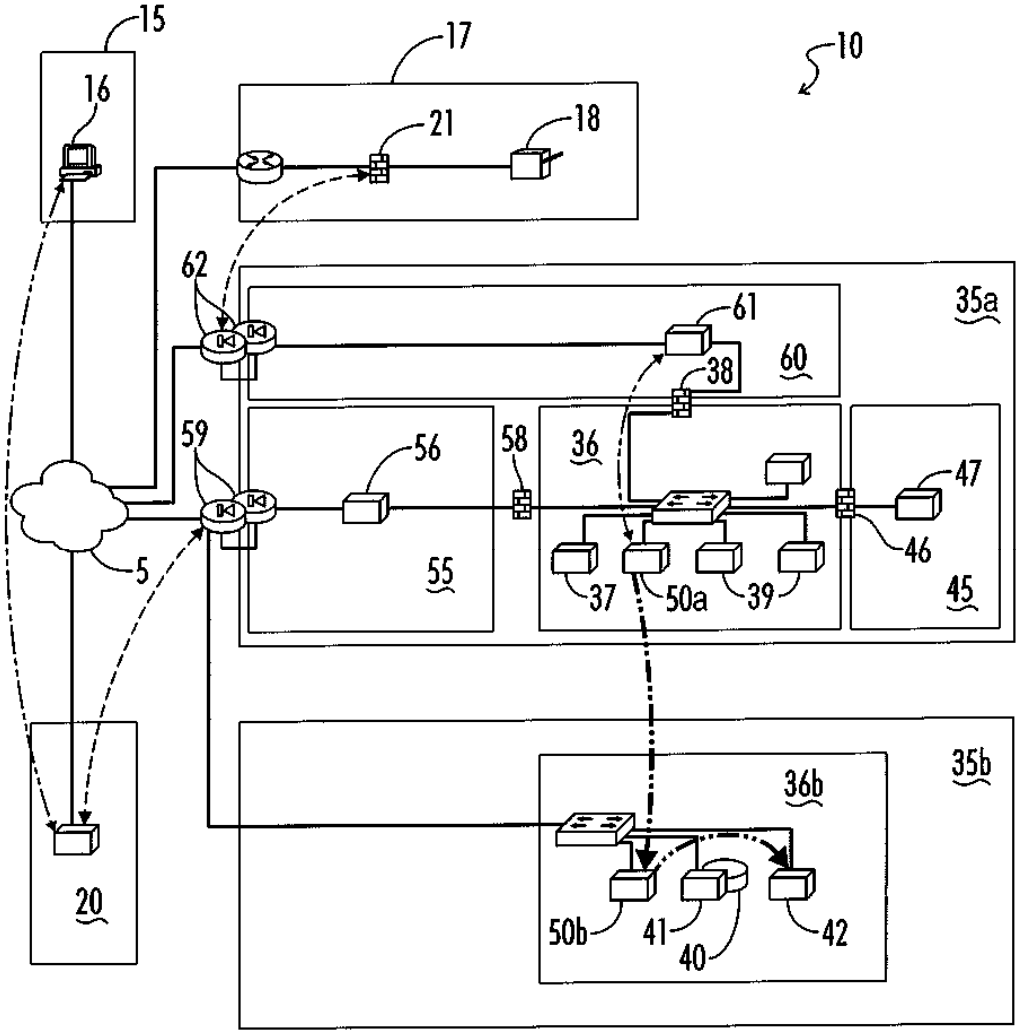
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
55
46
45
5
37
50a
39
35b
36b
20
50b
41
40
42

FIG. 3n

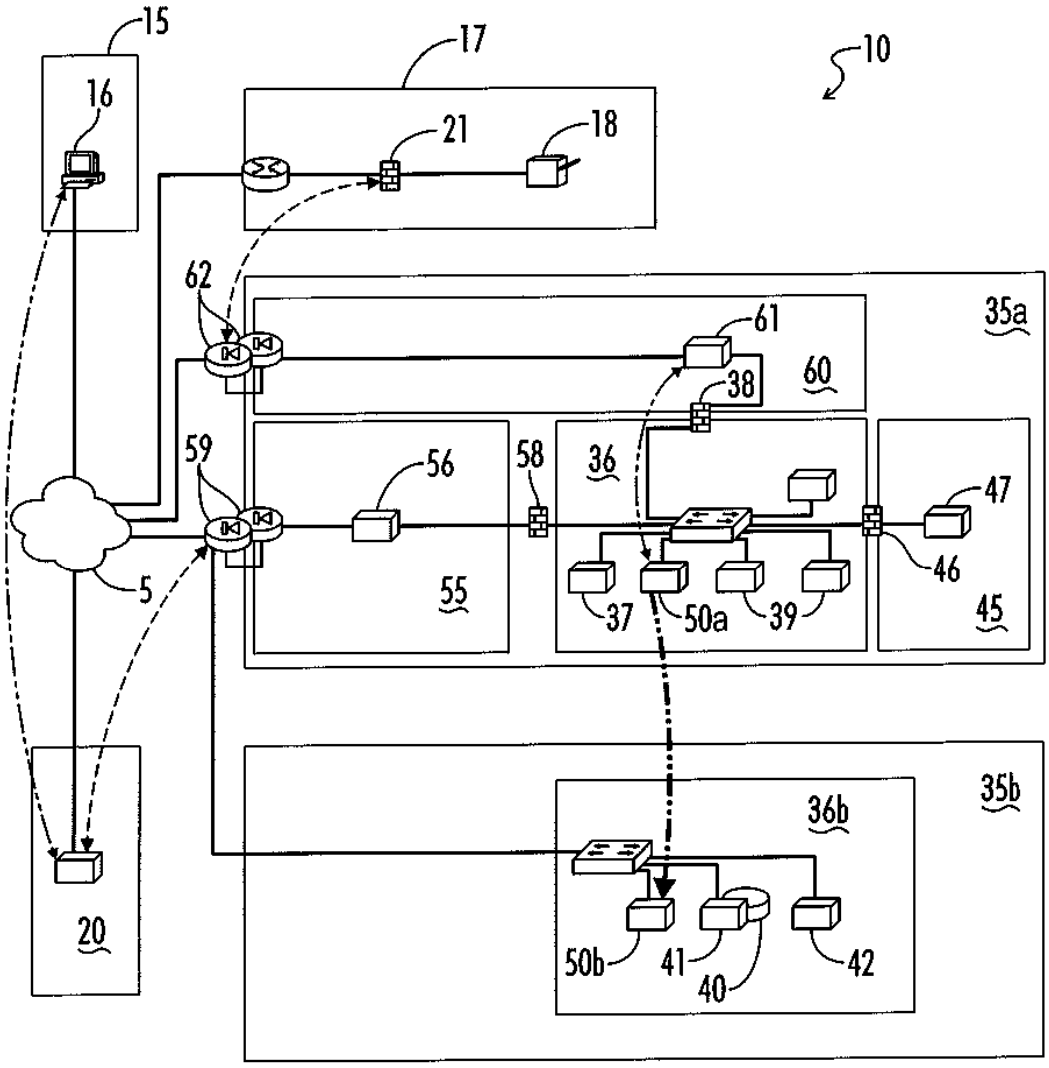
15
16
17
18
21
10
62
61
35a
60
38
59
56
58
36
47
55
46
45
5
37
50a
39
35b
36b
20
50b
41
42
40

FIG. 3o

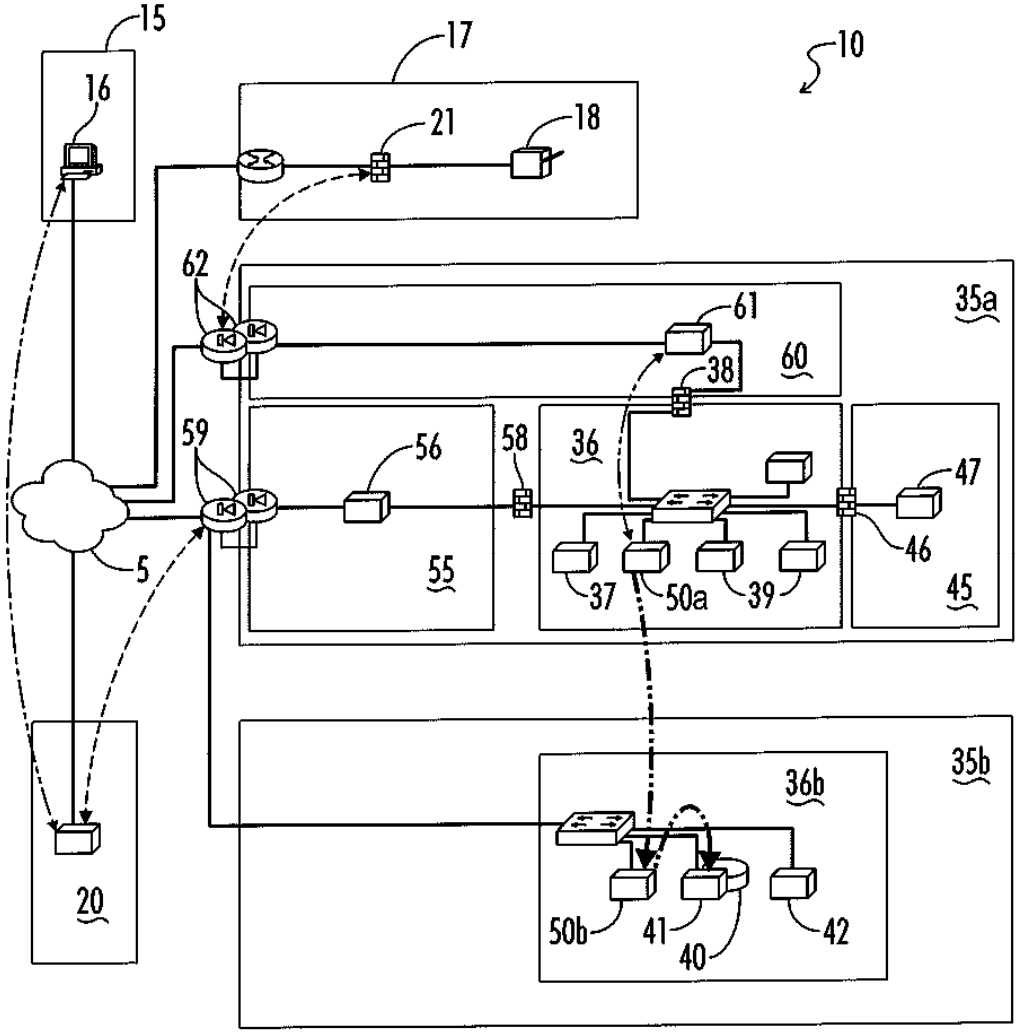
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
55
46
5
37
50a
39
45
35b
36b
20
50b
41
42
40

FIG. 3p

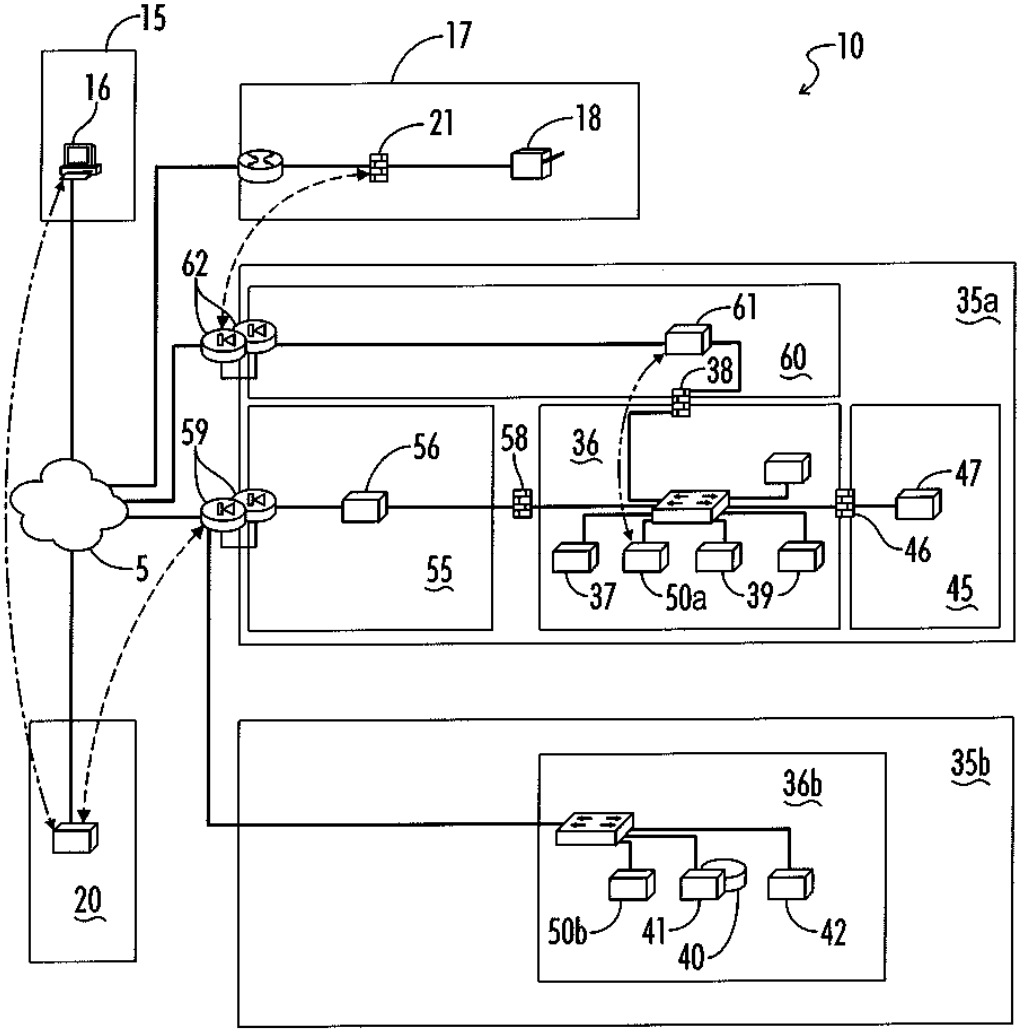
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
55
46
5
37
50a
39
45
35b
36b
20
50b
41
42
40

FIG. 3q

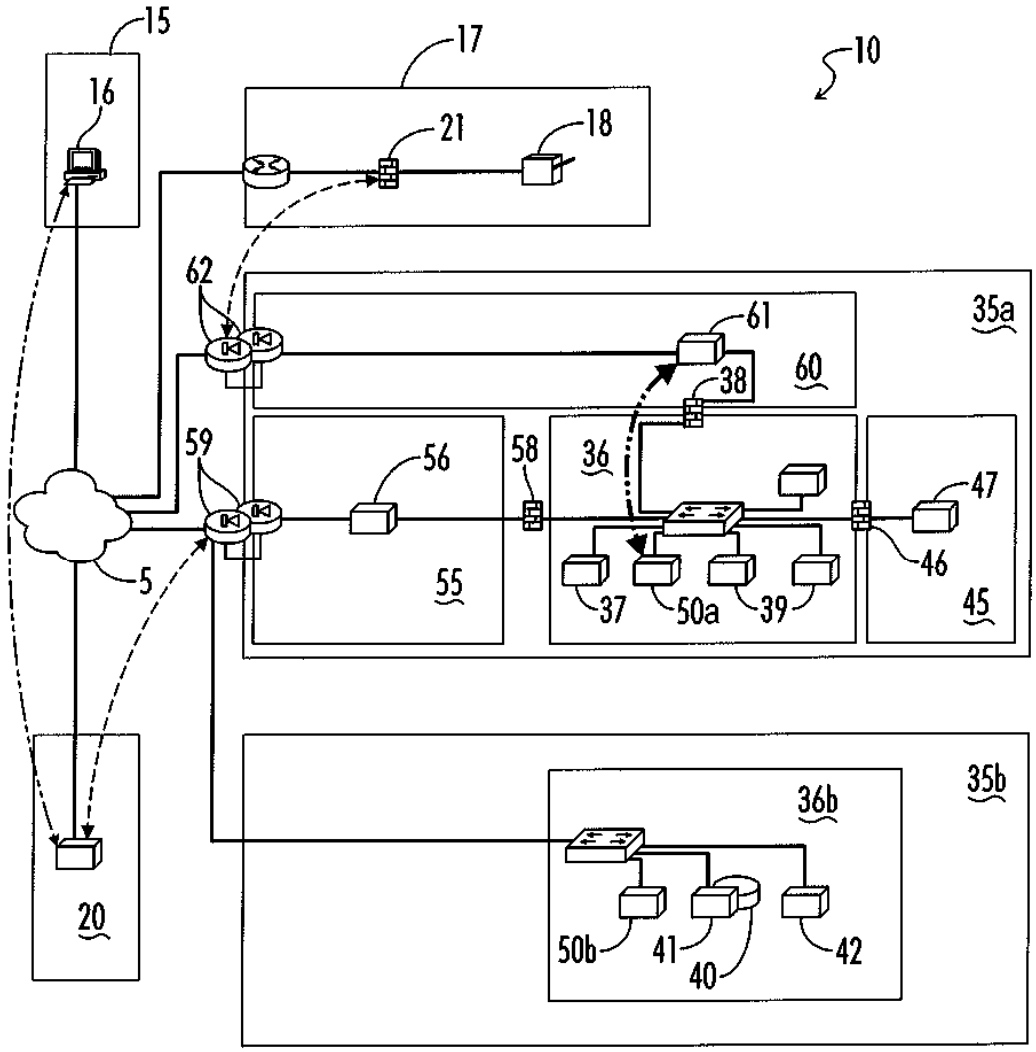
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
55
46
5
37
50a
39
45
35b
36b
20
50b
41
42
40

FIG. 3r

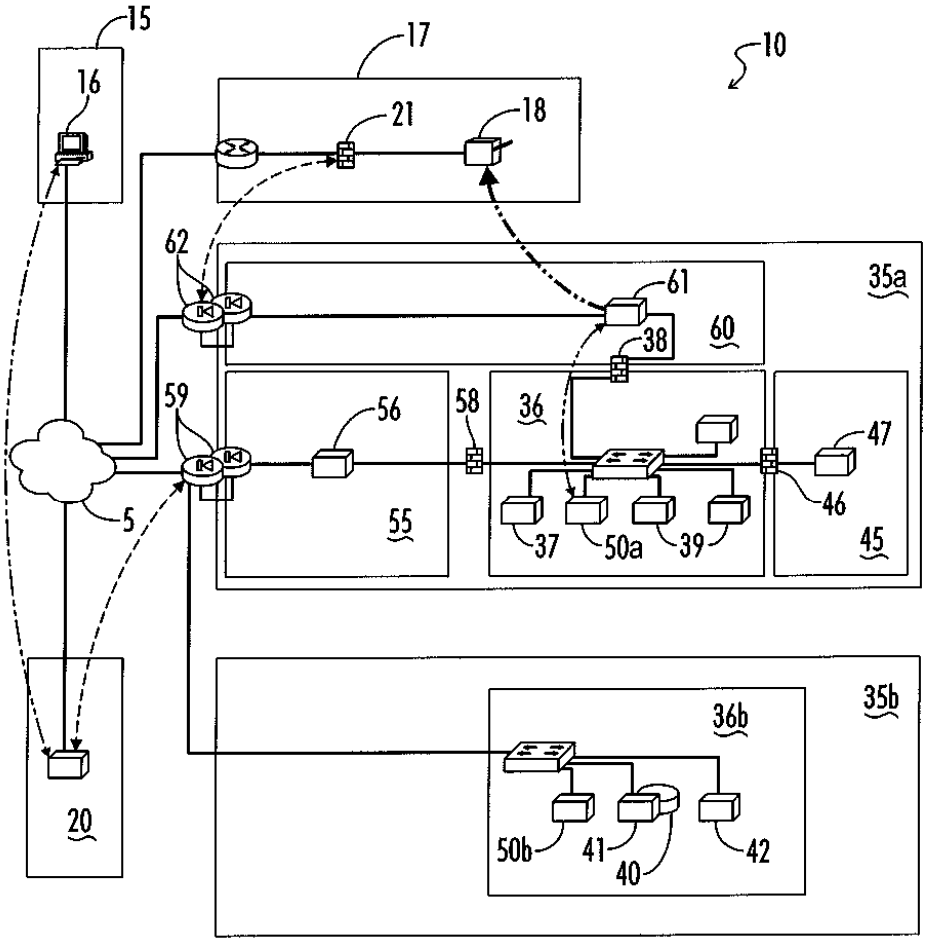
15
16
17
10
21
18
62
61
35a
60
38
59
56
58
36
47
5
55
37
50a
39
46
45
35b
36b
20
50b
41
40
42

FIG. 3s

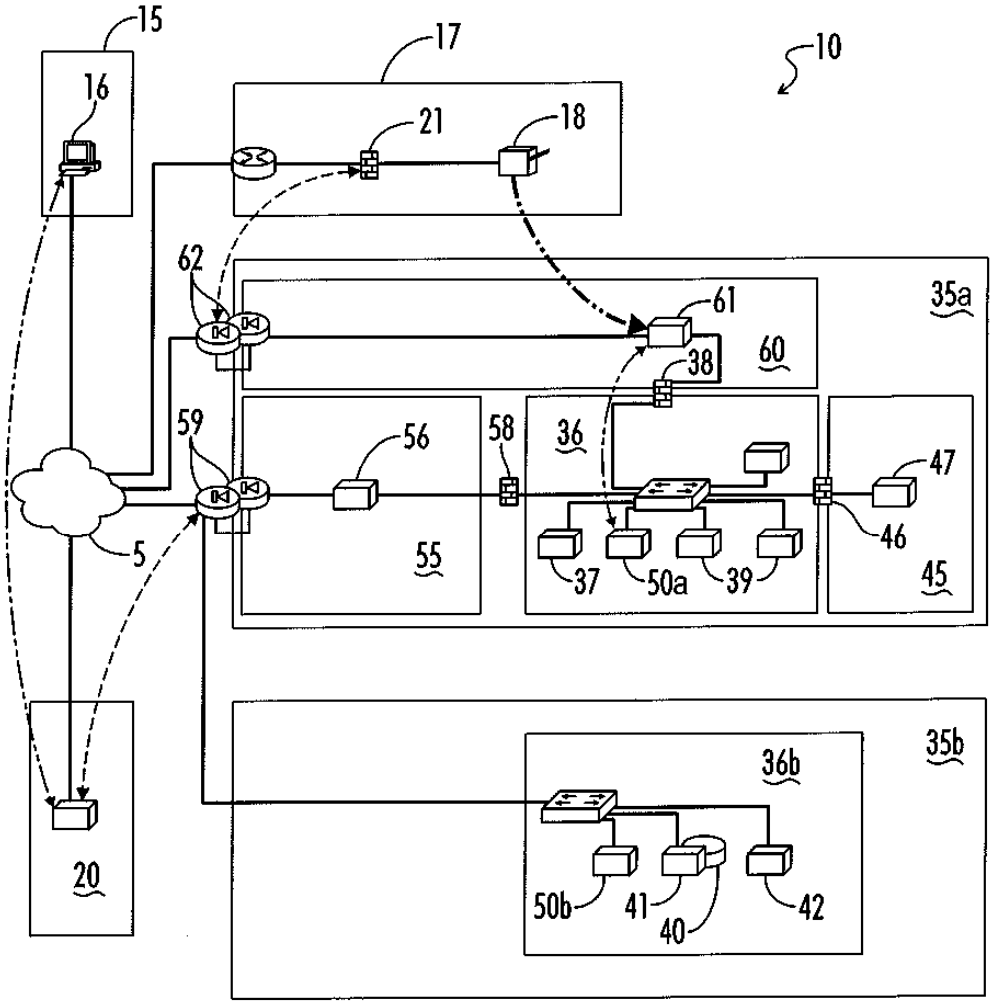
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
46
5
55
37
50a
39
45
35b
36b
20
50b
41
40
42

FIG. 3t

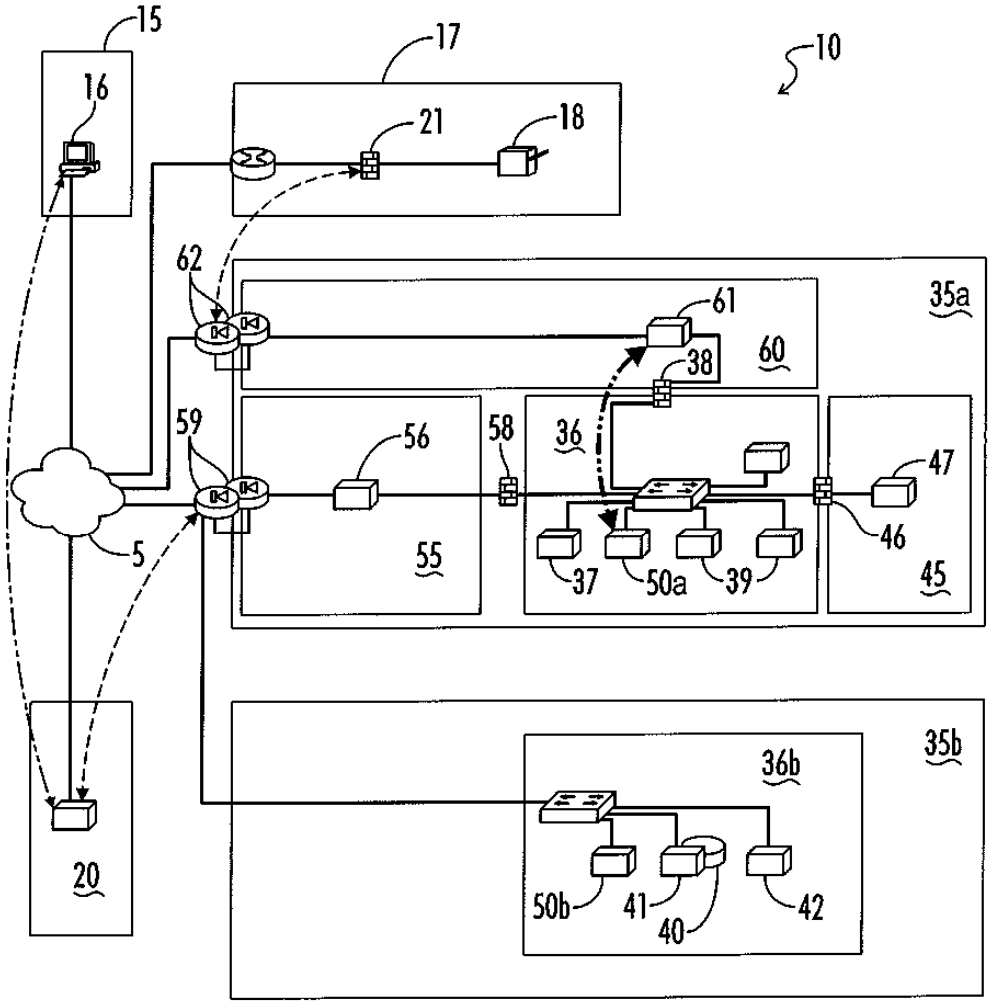
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
5
55
37
50a
39
46
45
35b
36b
20
50b
41
40
42

FIG. 3u

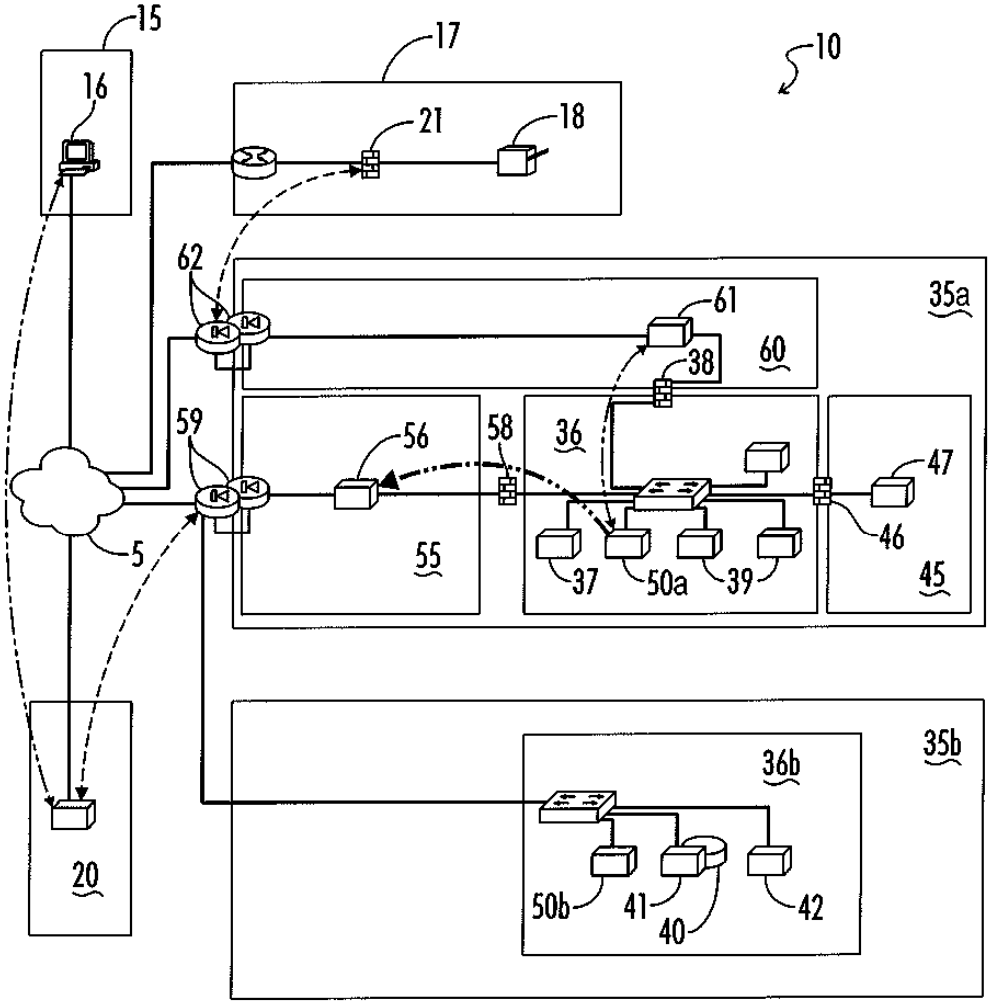
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
5
55
37
50a
39
46
45
35b
36b
20
50b
41
40
42

FIG. 3v

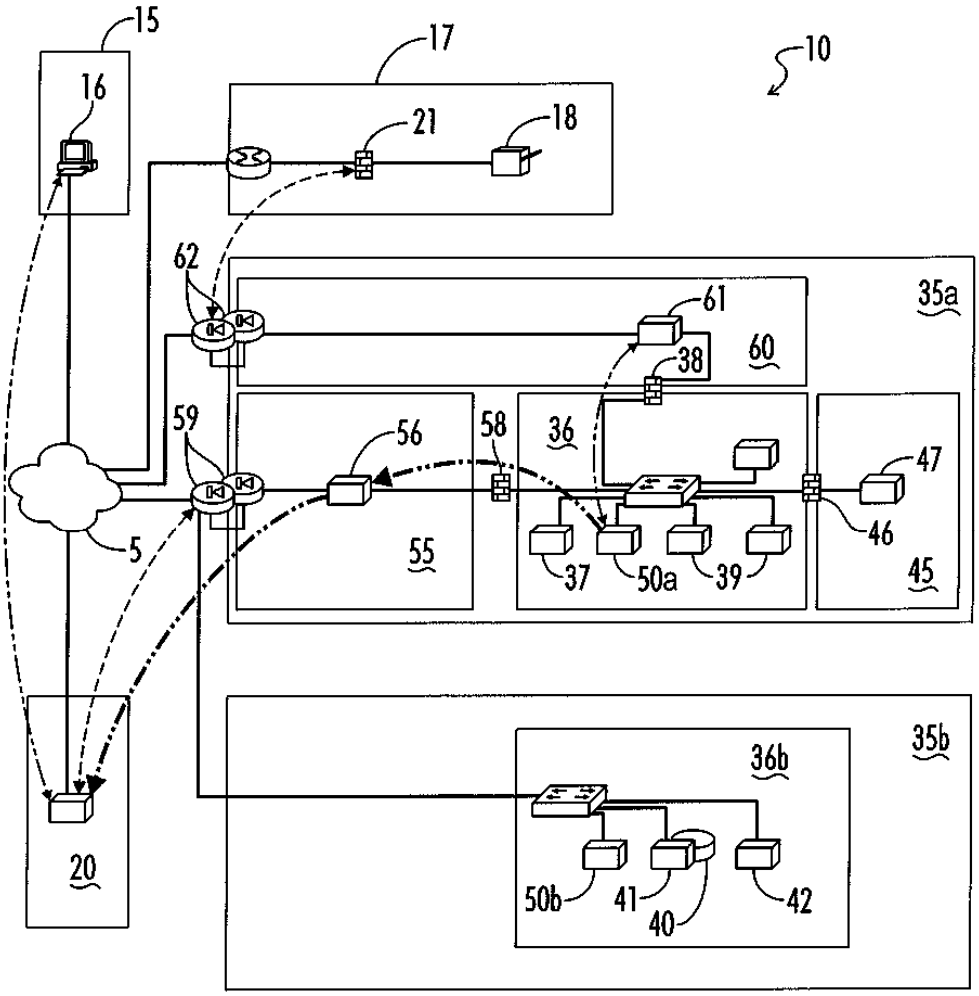
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
5
55
37
50a
39
46
45
35b
36b
20
50b
41
40
42

FIG. 3w

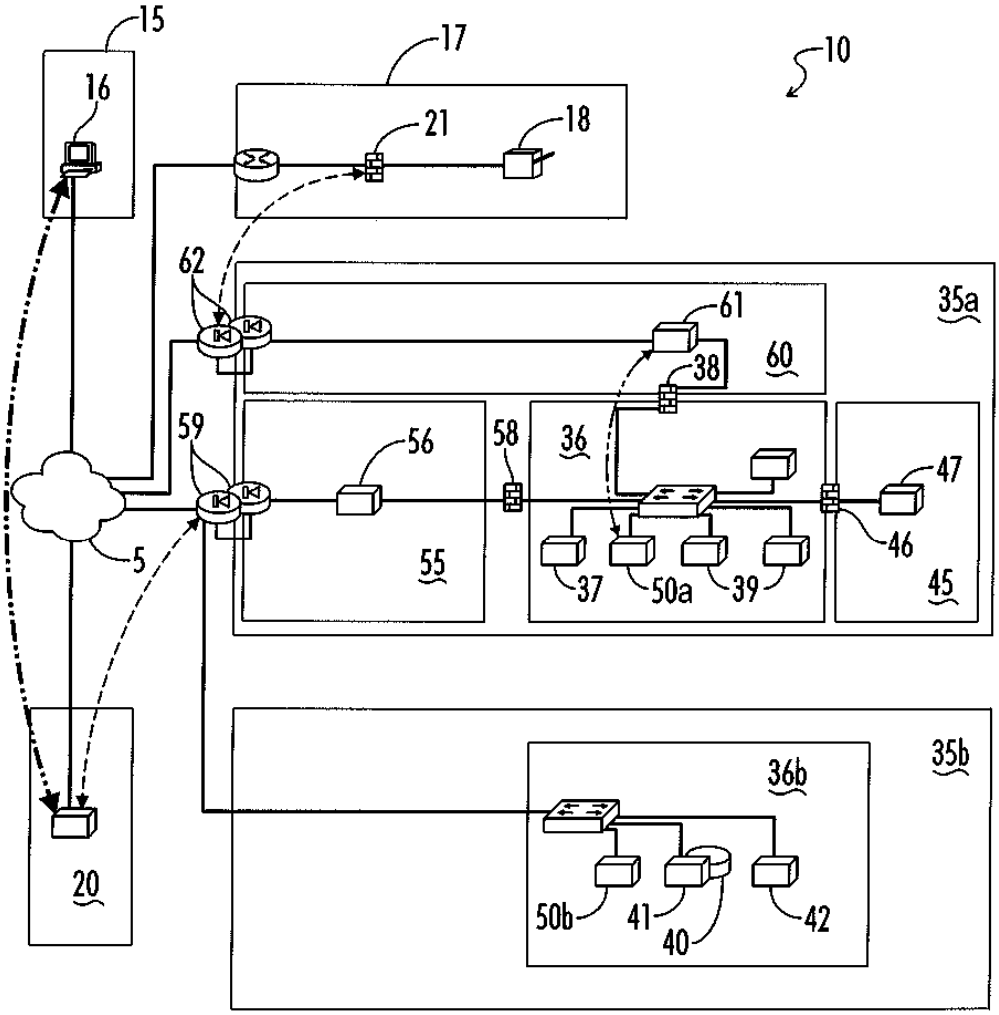
15
16
17
21
18
10
62
61
35a
60
38
59
56
58
36
47
5
55
37
50a
39
46
45
20
35b
36b
50b
41
40
42

FIG. 3x