FACTORES DE RIESGO QUE INFLUYEN EN LA INOPERATIVIDAD DE LAS REDES PRIVADAS VIRTUALES CON TECNOLOGÍAS FRAME RELAY Y X.25.

Beatriz J. Perozo S.
Universidad Rafael Belloso Chacín. Venezuela.

RESUMEN

El propósito de este estudio fue determinar cuales son los factores principales de riesgos Internos, externos y administrativos que influyen en la inoperatividad de las Redes Privadas Virtuales bajo la plataforma Frame Relay y X.25, El tipo de investigación es de campo y descriptiva, y la modalidad corresponde a Proyecto Factible, bajo el criterio del diseño no experimental. La población estuvo integradas por los Cinco (5) expertos que laboran en el departamento de Informática y Telecomunicaciones de la mencionada empresa. Se utilizó como instrumento de medición cualitativa la entrevista, cara a cara, informativa y estructurada, debido a la naturaleza del instrumento fue necesario utilizar para el tratamiento de la información un esquema no convencional, la cual requirió además de la validación de los expertos. Otra de las técnicas de recolección que se utilizó fue la Observación, no estructurada, participante e individual. Los resultados obtenidos identificaron factores de riesgo que atenta con la interoperatividad de las redes privada virtuales con las tecnologías antes mencionadas, a nivel de infraestructura de interconexión, Indicadores de rendimiento, factores administrativos, estos últimos evidencian que el incumplimiento de los contratos por parte de los proveedores de servicios (Carrier). También se convierten en una amenaza directa que incide en la inoperancia de la red, pues lo ideal seria el intercambio de información, sin interrupción ni errores y en tiempo real, que es lo que a ciencia cierta requiere toda organización.

Palabras clave: Factores de riesgos, Redes Privadas Virtuales, Tecnologías Frame Relay y X.25

ABSTRACT

The purpose of this study was to determine which are the main factors of Internal, external and administrative risks that affect in the operability of the Virtual Private Nets under the platform Frame Relay and X.25, The investigation type it is of field and descriptive, and the modality corresponds to Feasible Project, under the approach of the non experimental design. The population was integrated by the Five (5) experts that work in Computer science's department and Telecommunications of the mentioned company..

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 2 Edición No 2 – Año 2003

You uses like instrument of qualitative mensuration the Interview, face to face, informative and structured, due to the nature of the instrument you/he/she was necessary to use for the treatment of the information a non conventional outline, which required besides the validation of the experts. Another of the gathering techniques that was used was the Observation, not structured, participant and singular.. The obtained results identified factors of risk that attempts before with the operability of the virtual deprived nets with the technologies mentioned, at level of interconnection infrastructure, yield Indicators, administrative factors, these last ones evidence that the no fulfillment of the contracts on the part of the suppliers of services (Carrier) they also become a direct threat that impacts in the operative continuity of the net, because the ideal thing serious the exchange of information, without interruption neither errors and in real time that is what requires all organization to certain science.

Keywords: Factors of risks, Virtual Private Nets, Technologies Frame Relay and X.25.

OBJETIVOS DE LA INVESTIGACIÓN

El Objetivo principal de esta investigación es determinar cuales son los factores de riesgos internos, externos y administrativos que influyen en la interoperatividad de las redes privadas virtuales con tecnologías Frame Relay y X,25. Para cumplir con dicho objetivo se analizó la infraestructura de telecomunicaciones de la empresa HidroFalcón C.A. Ubicada en el la ciudad de Coro, así como también se evaluó el rendimiento de la red para detectar las fallas mas comunes que afectan la integridad de la transmisión de la data.

Finalmente se identificaron los factores de riesgos que atentan con la continuidad operativa de la Red Privada Virtual.

ANTECEDENTES

Para llevar a cabo la investigación es necesario indagar estudios realizados relacionadas con la variable objeto de estudio, para efecto de esta investigación los antecedentes son los siguientes:

FLORES MONTIEL, Henry Alessandro. Universidad Rafael Belloso Chacin.Tesis de grado. (2000) “Optimización de una red de transporte de telecomunicaciones.

El presente trabajo se realizó con la finalidad de evaluar la red de transporte de telecomunicaciones de la ciudad de Maracaibo, determinado el

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 2 Edición No 2 – Año 2003

rendimiento de la red identificando los aspectos que determinen la optimización de la red, así buscar mejorar la calidad del servicio del cliente en la empresa CANTV. Los factores de rendimiento son el Análisis de la estructura física de la Red y sus interfaces, la Velocidad de acceso para la transmisión de la información en tiempo real, Ancho de Banda de la trama, Tipo de tráfico y de caudal, Gestión de la red. Soporte del servicio, Encaminamiento en caso de fallos, Facilidad de Gestión de clientes entre otros. Evidentemente todos estos factores de rendimiento, midieron el nivel de cuantificación de la calidad del servicio, y a su vez permitieron determinar los puntos críticos de la red, y ofrecer diferentes soluciones alternas obtener un incremento del nivel de calidad a la CANTV como empresa líder en telecomunicaciones.

HUNG V. Fermin. Universidad Rafael Belloso Chacin. Tesis de grado. (2001) "Red Privada de Servicios Integrados para la interconexión de un ente corporativo gubernamental".

El propósito de este estudio, fue diseñar un modelo de interconexión para todas sus dependencias gubernamentales con una red rápida, sencilla, segura y asequible. Para realizar este modelo se diseño un esquema lógico de la red, para evaluar cual era la tecnología mas idónea que soportaría la red. Este proyecto de investigación, realizara un aporte significativo que permitirá comparar el diseño lógico de la Red Privada Virtual para un ente gubernamental y el adoptado por la empresa Hidrofalcón C.A, a fin de identificar debilidades en la estructura de la red que utiliza dicha empresa como medio de transmisión de sus transacciones comerciales.

ROO, Avigdys. Universidad Rafael Belloso Chacin. Tesis de grado. (2001) "Red privada Virtual como alternativa para el acceso remoto".

El presente trabajo se desarrolló con la finalidad de implementar una red privada virtual como alternativa para proporcionar a las empresas como a sus usuarios remotos acceso electrónico y otros recursos de la red. Para lograr esta funcionalidad, la tecnología de redes seguras y virtuales se debe completar las siguientes tareas: Capacidad de pasar paquetes IP a través de un túnel en la red pública, de manera que dos segmentos de LAN remotos no parezcan estar separados por una red publica, agregar encriptación, de manera que el tráfico que cruce por la red pública no puede ser copiado o interrumpido, leído o modificado por personas no autorizadas, y autentificar cualquier extremo del enlace de comunicación, de modo que un adversario no pueda acceder a los recursos del sistema.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 2 Edición No 2 – Año 2003

URDANETA V. Marcos A. Universidad Rafael Belloso Chacin. Tesis de Grado. (2001) "Modelo de interconexión segura basada en la tecnología de Red Privada Virtual (VPN)".

El propósito de ese estudio, fue diseñar un modelo de interconexión segura utilizando como mecanismo de seguridad la Red Privada Virtual (VPN), de esta manera permitirá al usuario utilizar red basada en IP, para el acceso seguro a Intranet, Extranet y acceso remoto, facilitando a las empresas comparar soluciones eficaces a nivel de costes, basadas en una Red Publica segura, que transmita información totalmente confidencial, auque el transporte se realice a través de una Red Pública, prescindiendo de las redes corporativas convencionales dedicadas y con unos coste de explotación superior.

CONSIDERACIONES TEORICAS

Las bases teóricas utilizadas como soporte conceptual para la presente investigación abordan aspectos generales relacionados con redes de telecomunicaciones, tecnologías, entre otros.

Según Tanenbaunt (1998), una **red de telecomunicaciones** esta formada por los sistemas de transmisión y, cuando proceda, los equipos de conmutación y demás recursos que permitan la transmisión de señales entre puntos de terminación definidos mediante cables, medios ópticos o de otra índole.

Y sus **Objetivos** garantiza servicios de comunicaciones, de muy diversas naturalezas, a los usuarios que se conecten a ellas, como el de Ofrecer en sus transmisiones voz, datos e imágenes con la calidad, asi mismo, permite la integración de las redes y la convergencia de servicios hacen que el usuario no se tenga que preocupar de a donde o como esta conectado. Según González (1987) **X.25** es una red de comunicación de datos que trabaja dentro de la 3 primeras capas del modelo OSI (Open System Interconnection), Capa Física, capa de Enlace de datos y Capa de Red, y maneja un conjunto de normas asociadas para la conexión de equipos asincronos y para la conexión de otras redes, utilizando la conmutación de paquetes (tramas) para lograr la transmisión de datos. Existen dos posibilidades a la hora de acceder a una red de conmutación de paquetes X.25:

1.- Acceso Dedicado: Mediante una línea punto apunto el usuario se conecta al nodo más cercano, a la velocidad de acceso elegida.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 2 Edición No 2 – Año 2003

2.- Acceso por red conmutada: Mediante el empleo de un módem y por RTC, los usuarios se conectan a la red X.25, pudiendo utilizar terminales en modo paquete o asincronos, necesitando en este ultimo caso un PAD.

Suárez. (2000). Asegura que, **Frame Relay** es una alta tecnología de conmutación de tramas o paquetes, basadas en estándares internacionales que puede utilizarse como protocolo de acceso, se usa principalmente para la interconexión de redes de área local y redes de área extensa sobre redes publicas y privadas. Además de los dispositivos de interconexión que utiliza esta tecnología, como lo son: Computador Personal, Host de la Red, Equipos de comunicaciones de Datos(DTE), Equipos terminales de Datos(DCE).

Frame Relay opera con el supuesto de que las conexiones son confiables y transporta únicamente datos. Elimina gran parte del control y detección de errores de X.25, por lo que requiere de menos procesamiento de este. Soporta velocidades en el rango de 256 Kbps a 24 Mbps. La transmisión se los datos desde un terminal son encapsulados sobre un paquete frame Relay, La dirección del destinatario esta junto al paquete de Frame Relay con los datos sobre el apropiado circuito virtual, Frame Relay no hace correcciones de errores, Los paquetes dañados son descartados. Pero si la red esta congestionada los paquetes pueden ser descartados.

Entre la implicaciones del Frame Relay, El equipo terminal debe ser inteligente y hacer correcciones de errores; Requiere de poco procesamiento, Menor complejidad en equipamiento, lo cual significa menores costos en fabricación de equipos y, Transporta datos dentro de la trama y no maneja paquetes, tiene la capacidad de realizar funciones de enrutamiento a nivel de Frame.

La tecnología **Frame Relay** se basa en el uso de circuitos Virtuales, los cuales son caminos de datos de doble vía, definidos sobre el software entre dos puertos que actúan sobre líneas privadas de la red. Existen dos tipos de conexiones; Los **Circuitos Virtuales permanentes** (PVC), son inicialmente definidos como una conexión entre dos sitios. y establecidos por el operador de la red de un sistema de administración de red. Por tanto, los PVCs son como un circuito. Dedicado punto a punto. Y los **Circuitos Virtuales Conmutados** que están disponibles para una base de llamada por llamada. Implementar SVCs en la red es mas complejo que usar PVCs, pero es transparente para los usuarios. Los beneficios que ofrece la tecnología **Frame Relay**, permite al usuario aprovechar al máximo cualquier mejora cualitativa en la capa Física del modelo OSI. Además ofrecerá; Un bajo costo, ya que la inversión no depende del trafico, Amplia gama de conexiones lógicas sobre una simple línea de acceso, Manejo con eficiencia

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 2 Edición No 2 – Año 2003

el trafico irregular e impredecible, Soporte múltiples de protocolos y necesita menos equipos con pocos puertos, Soporta fácilmente ambientes de malla, y permite un rápido desarrollo de redes digitales.

Según, Jentjens. (2000). **Una red privada virtual** es aquella que conecta los componentes de una red sobre otra red. Esto permite que el usuario haga un túnel a través de Internet u otra red pública, de manera que permita a los participantes del túnel disfrutar de la misma seguridad y funciones. Por lo general, al implementar un solución de red remota, una compañía desea facilitar un acceso controlado a los recursos y a la información de la misma. La solución deberá permitir la libertad para que los clientes remotos autorizados se conecten con facilidad a los recursos corporativos de la red de área local (LAN), así como que las oficinas remotas se conecten entre sí para compartir recursos e información.

Por lo tanto, una solución de VPN debe proporcional como mínimo La Autenticación del usuario, para verificar la identidad del mismo y restringir el acceso de la VPN a usuarios autorizados; La Administración de la dirección la asignara una dirección al cliente en la red privada, y asegurarse que las direcciones se mantengan así; La Encriptación de datos, la cual garantiza que los datos que viajan en una red pública no podrán ser leídos por clientes no autorizados en la red, esto atenta contra la integridad de la data; La Administración de la llaves para generar y renovar las llaves de encriptación para el cliente y para el servidor, y por ultimo el Soporte del protocolo múltiple para manejar protocolos comunes utilizados en las redes publicas, es incluyen el protocolo de Internet Central de paquetes de Internet.

ANÁLISIS DE LOS RESULTADOS

Después de haber medido periódicamente el rendimiento de la red, utilizando como herramienta el **Análisis Baseline,** diseñada para proporcionar un diagnostico de la infraestructura de redes y sistemas con un visión métrica clara y objetivas. Por medio de este análisis se determinaron los factores de riesgo que se identificarán a continuación:

Factores Internos: Involucran directamente el funcionamiento de la red como; al no tener una distribución adecuada de la red que permita el balanceo de las carga sobre los dispositivos de interconexión. Esto se evidencia al detectar alarmas criticas de sobrecarga de red, ocasionando colisiones de sus paquetes y por ende la perdida de información; Esto se dá cuando una estación quiere conectarse generando una tormenta de Broadcast, indicando que existe un problema de Interconectividad.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 2 Edición No 2 – Año 2003

Otros factores que generan fallos a la red son; La instalación de Varios protocolos, La ubicación de concentradores en cascadas, asignación de todos los puertos sin Holgura, configuración inadecuada de los servidores , del cableado estructurado, y del nivel de Software y Hardware.

La Administración de los recursos humanos y financieros, es otro de los factores internos que obstaculizan la operatividad de la red. Este involucra la inexistencia de un plan de adiestramiento y actualización técnica del personal, la factibilidad técnica y operativa no disponible, la demora en el proceso licitatorio para proveedores de servicios y la resistencia a los cambios en la red por parte de la organización.

Factores Externos; Entre los entes exógenos que atenta con la continuidad operativa de red se evidencia: El incumplimiento de contratos por parte del proveedor de servicios, los cambios sustanciales de las normativas de CONATEL, que afectan las concesiones de los proveedores y, la futura obsolescencia de la plataforma de telecomunicaciones.

CONCLUSIONES Y RECOMENDACIONES

El primer paso para la administración de una red consiste en documentarla y para ello es necesario realizar las auditorias pertinentes. Para evaluar la **infraestructura de la red privada virtual** se realizará una **auditoria de Inventario** que identifique todos los elementos de software y hardware instalados en la red, que asegure que el numero de usuario no supere la cantidad de licencia y, determine la cantidad de dispositivos de interconexión requeridos. La **Auditoria de instalaciones** suministra información de todos los componentes de la red (cableado, estaciones de trabajos, dispositivos de interconexión). Esta auditoria debe estar soportada por un mapa de red que ayude a detectar rápidamente fallos en la misma.

Por otra parte, se debe medir el **rendimiento de la red privada virtual** por medio de: **Auditorias de Funcionamiento**, que permite observar las operaciones diarias de la red utilizando herramientas de administración de hardware y software especializadas, detectando interrupciones en el servicios, ruido en los medios, cuellos de botellas, circuitos en los cables, este ultimo se debe al incumplimiento de las normas del instituto de ingeniería eléctrica y electrónica (IEEE). Otro aspecto involucrado es la **Auditoria de Eficiencia,** que permite determinar si la red está funcionando de acuerdo con su potencial de trabajo. Esto incluye un análisis de costo, de factibilidad y de capacidad, que indique si la red puede recuperar información y garantizar la integridad de los datos.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 2 Edición No 2 – Año 2003

Y por ultimo la **Auditoria de Seguridad** analiza los requisitos de seguridad y la forma en que la red y los clientes usan y acceden a los datos.

Por otra parte, se puede contribuir en pro del mejor desempeño de la red, asumiendo una conducta positiva frente al cambio de nuevas tecnologías, la organización debe incluir dentro de sus políticas el desarrollo de proyectos futuros de expansión a cambios en las redes, ajustándose siempre a las normas presentadas por el ente regulador de las telecomunicaciones de Venezuela CONATEL

REFERENCIAS BIBLIOGRAFICAS

Aguirre, P. (2002, Marzo 20): Factores que afectan la operatividad de las Redes Privadas. Entrevista Personal. Empresa Hidrofalcón. Coro.

Angelfire. Redes X.25. [1998] [En Linea]. http:www/angelfire.com/wi/ociosonet/s.html. [2002. Marzo 20].

Blanco, M. (2000). Las Telecomunicaciones como Actividad Económica de Interés .General. Inversiones.(206), 20-25.

Ballestrinni, M. (1998). Cómo se elabora el Proyecto de Investigación. Venezuela. Consultores Asociados BL. Servicios Editorial.

Cisco Press (2001). Academia de networking de Cisco System. Guía del primer año.

ConsulTel (1997). Frame Relay. [En línea] http://www.consulintel.es/html/tutoriales/frf.html. [2002. Abril 11]

Derfler, F. (1997). Descubre redes LAN & WAN. España. Prentice Hall.

Dyson, P. (1997). Diccionario de Redes. Santa Fe Bogota. MacGraw-Hill.

García, E. (2002, Abril 12).Infraestructura de Interconexión de Redes Frame Relay y X.25. Entrevista Personal. Empresa Hidrofalcon. Coro.

González, N.(1987). Comunicaciones y Redes de Procesamiento. México. MacGraw-Hill.

Held, G. (1998). Diccionario de tecnología de las comunicaciones. México. Paraninfo

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 2 Edición No 2 – Año 2003

Halsall, F (1998). Comunicación de Datos, Redes de Computadores y Sistemas Abiertos. Cuarta Edición. EEUU. Addison – Wesley Iberoamericana.

Huidobro , J. (2000). Redes y Servicios de Telecomunicaciones. México. Paraninfo.

Hurtado, R.(2002). Informe de Asistencia Técnica. Trabajo no publicado. Compañía Anónima de Teléfonos de Venezuela (CANTV).

Ictnet. (2000). Construyendo Redes Privadas Virtuales en Internet. [En línea]. Ictnet.http://www.ictnet.es/ [2002, Febrero 12).

Interec (2000). Conexion Frame Relay. [En Linea]. http://www.interec.com/frame_relay/cfr3.html. [2002, Febrero 12]

IPS. Redes Privadas Virtuales. [En Línea].
http://www.ips.es/ RPSV.htm>.[2002, Marzo 15].

Jentjens, K. (2000). Redes Privadas Virtuales. PC Magazines en Español.(8). 16-25.

Martínez, A. (1998). *GS* Comunicaciones. España: Paraninfo

Molina, K. (2001). Proyecto Red Privada Virtual Hidrofalcón. Trabajo no publicado. Empresa Hidrofalcón.

Peña, J. (1999). Comunicaciones de Datos. México. Editorial Paraninfo.

Stanlling, W. (1997). Comunicaciones y redes de computadoras. España. Prentice- Hall.

Suárez, V. (2000). La Apertura de las Telecomunicaciones .Inversiones. (205).10-14.

Symantec. Estudio Preliminar de las VPN. [En Linea]. Symantec. <http://ucnet.com.mx/dialup/remoto.html>. [2002, Marzo 12].

Urdaneta, M. (2001). Modelo de Interconexión segura basada en la tecnología VPN. Tesis de Maestría en Telemática. Universidad Dr. Rafael Belloso Chacin. Maracaibo. Venezuela.

Tanembaum, W. Redes de Computadoras (1998). España: MacGraw - Hill.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 2 Edición No 2 – Año 2003