ManageEngine
NetFlow Analyzer

Gestión del tráfico de red empresarial

Resumen

En este documento se destaca la importancia de contar con una herramienta de análisis de tráfico de red para toda la empresa en las empresas globales actuales. Al aprovechar los datos contenidos en las exportaciones de flujo (NetFlow, sFlow, CFlow, J-Flow, NetStream e IPFIX) desde routers y switches, puede obtener información detallada sobre el tráfico de su red, incluido el "quién, qué y por qué" del uso del ancho de banda.

Esta información es vital para que los responsables de TI tomen las decisiones estratégicas correctas que puedan beneficiar a toda la organización. En este documento se analizan las ventajas de implementar una solución de software basada en flujo que utiliza la recopilación distribuida. A diferencia del hardware, que utiliza monitoreo basado en probes, una solución de software basada en flujo requiere menos inversión, es fácil de instalar y aporta valor en cuestión de horas.

Tabla de contenido

1.El fin de los negocios tal como los conocemos

En el cambiante panorama empresarial actual, las redes informáticas desempeñan un papel vital. Los negocios ya no se limitan a las cuatro paredes de la empresa. Para ser competitivas, las grandes empresas de hoy en día necesitan seguir estrategias como offshoring, outsourcing, smart-sourcing, etc. Implementar estas estrategias globaliza la naturaleza del trabajo, lo que significa que el trabajo se realiza en varias geografías y zonas horarias. ¡Bienvenido a la empresa distribuida!

[IMAGEN:

Centro de datos	Oficina central	**Ventas y marketing**		
			Centro de I+D	**Ventas y marketing**
	Centro de llamadas	Sucursal		Sucursal

]

Las empresas de hoy en día están adoptando algunas de estas estrategias:

- Es habitual que las empresas tengan su sede en el Reino Unido; los proveedores de materias primas (cadena de suministro) en China, Brasil y Noruega; la mano de obra especializada en la India; y el personal de ventas y marketing distribuido en todo el mundo. También es común que gran parte de sus ventas se realicen a través del comercio electrónico.

Para evitar problemas legales y cumplir con el creciente número de normas sobre integridad y seguridad de los de datos (como HIPAA, SOX y similares), las empresas hoy en día prefieren tener toda su base de datos para todos los aspectos de su negocio en un centro de datos seguro y central, principalmente con sede en los Estados Unidos.

- Para cubrir el costo asociado con la implementación de administradores de red calificados en varias oficinas distribuidas y también para superar el desafío de encontrar personal calificado, las empresas prefieren monitorear sus redes globales de forma centralizada.
- Todas las empresas que desean reducir costos y seguir siendo competitivas están eliminando los costos asociados con la adquisición de software y aplicaciones patentadas. La tendencia emergente es que las empresas se están moviendo hacia el modelo de software como servicio (SaaS). Esto incluye el uso de aplicaciones web como Salesforce.com para la automatización de la fuerza laboral de ventas, Zoho para la productividad empresarial, etc.
- Por ello, es crucial facilitar el acceso y la comunicación entre los diversos componentes de la red distribuida y garantizar el acceso al centro de datos/aplicación SaaS desde las oficinas remotas. Además, para monitorear toda la red desde una ubicación centralizada, se vuelve indispensable tener una vista unificada de toda la red.

En el cambiante panorama empresarial actual, las redes informáticas desempeñan un papel vital. Los negocios ya no se limitan a las cuatro paredes de la empresa. Para ser competitivas, las grandes empresas de hoy en día necesitan seguir estrategias como offshoring, outsourcing, smart-sourcing, etc. Implementar estas estrategias globaliza la naturaleza del trabajo, lo que significa que el trabajo se realiza en varias geografías y zonas horarias. ¡Bienvenido a la empresa distribuida!

2. Gestión del ancho de banda empresarial: Un requisito estratégico

Con los cambios de dominio de red que se están produciendo en las empresas en estos días, el administrador de red debe garantizar un alto nivel de disponibilidad de la WAN todo el tiempo. A medida que una empresa adquiere presencia global, se vuelve un desafío gestionar el estado y el rendimiento de toda la red, incluidas las oficinas remotas y sucursales.

Cualquier degradación en el rendimiento de la red en cualquier lugar de la red podría provocar una pérdida significativa de productividad y frustración de los empleados. Es aún más importante asegurarse de que no hay tráfico indeseado, abuso de la red o ataques a la red en cualquier momento.

Los principales desafíos en tal escenario incluyen:

1. Garantizar una sólida conectividad de red y una disponibilidad de ancho de banda constante. El ancho de banda no debe ser un factor limitante para el éxito de una empresa.
2. Garantizar un ancho de banda óptimo para aplicaciones críticas. Asegúrese de que las aplicaciones que generan ingresos tengan prioridad sobre las aplicaciones triviales. Priorice las aplicaciones críticas como el acceso a SAP HRMS, Oracle Financials, Zoho CRM y Salesforce.com, o el acceso al mainframe IBM de la empresa sobre cosas triviales como la transmisión de videos, la descarga de música, etc.
3. Solucionar rápidamente cualquier incidente de red, determinando la causa raíz de los problemas para solucionarlos rápidamente.

Planificar la capacidad de forma precisa, ya que los costos involucrados son altos para las grandes empresas.

4. Mantener un control de la red global.
    - Manténgase informado: ¿El ancho de banda de la red de su empresa se utiliza correctamente o no?
    - La falta de disponibilidad de administradores de red cualificados se puede superar proporcionando un monitoreo centralizado al administrador de red.
5. Garantizar que la calidad del servicio prestado por el ISP esté alineada con los términos del acuerdo.

La única manera de abordar estos problemas es contar con una potente herramienta de monitoreo de ancho de banda y análisis de tráfico en toda la empresa. Al tener información sobre los patrones de tráfico en departamentos similares en todas las oficinas y geografías y sobre los recursos que consumen ancho de banda, un administrador de red o CIO puede aplicar las políticas adecuadas para restringir el uso de ancho de banda no deseado, como descargar archivos de música o ver videos de YouTube durante el horario laboral. Esta visión unificada y colectiva del consumo de ancho de banda también ayuda a tomar decisiones estratégicas precisas sobre la planificación de la capacidad (solicitar más ancho de banda). Además, tener acceso a datos históricos del patrón de uso del tráfico ayuda a comparar los niveles de uso actuales.

3. Enfoques típicos para el monitoreo del ancho de banda

Hay varios tipos de soluciones de monitoreo de ancho de banda entre los cuales elegir. En general, se pueden clasificar en función de la tecnología subyacente (técnica de adquisición de datos).

Basado en la adquisición de datos

Las soluciones de monitoreo de ancho de banda suelen adoptar una de estas técnicas: consulta SNMP, puertos de acceso de prueba (TAP), puertos de análisis de puerto de switch (SPAN), rastreo de paquetes o análisis de exportaciones de flujo como NetFlow, sFlow, Cflow, J-Flow, NetStream e IPFIX.

La técnica de SNMP utiliza consultas SNMP en los agentes SNMP que se ejecutan en el dispositivo de red para obtener información sobre el uso del ancho de banda en la red. La consulta SNMP proporciona una cifra de tráfico consolidado o masivo. Por lo tanto, esto debe complementarse con un análisis exhaustivo del tráfico de red que responda preguntas como quién está usando qué ancho de banda y cuándo. Sin embargo, dado que SNMP utiliza la tecnología de extracción, puede terminar consumiendo una cantidad considerable del ancho de banda de su empresa.

Los puertos SPAN se designan en los switches para replicar el tráfico recibido en otros puertos. Los TAP son replicadores de tráfico ubicados entre dos routers, firewalls o switches empresariales que envían una copia de todo el tráfico de red que fluye a través de ellos. Los puertos SPAN y TAP se pueden utilizar para reenviar el tráfico de red a aplicaciones de software o probes de hardware para analizar el tráfico y obtener información sobre el tráfico de red. La desventaja es el costo involucrado en la adquisición, implementación y gestión de este tipo de puertos. Un rastreador de paquetes intercepta y recopila el tráfico local capturando los paquetes de la red a la que está conectado el rastreador.

Un rastreador se utiliza para resolver problemas de red, detectar intrusiones de red y monitorear el uso de la red mediante la visualización de información de tráfico real por dirección IP y protocolo. La desventaja es la carga pesada en el sistema de control.

La tecnología basada en flujo aprovecha la información contenida en las exportaciones de flujo como NetFlow, sFlow, Cflow, J-Flow, NetStream e IPFIX y presenta una vista detallada del flujo de tráfico. Ofrece un enfoque escalable y de bajo costo para tener una visión profunda del tráfico de red basada en la información de paquetes de capa 3 y capa 4. Con esta información, sabrá quién está usando qué ancho de banda y cuándo.

Utilizando los datos extraídos de los flujos, sabrá:

- Quiénes son los principales interlocutores de la red.
- Cuando el tráfico alcanza su nivel máximo y por qué.
- Durante cuánto tiempo se produce un pico en el uso del ancho de banda y por qué.
- El origen y destino implicados en una conversación.

Este enfoque proporciona la información necesaria para tomar decisiones de planificación de capacidad, detectar cualquier forma de abuso de red en el monitoreo de QoS y, en cierta medida, identificar ataques de seguridad.

La siguiente tabla muestra el tipo de flujo para los siguientes proveedores.

Tipo de flujo	**Dispositivos de proveedores compatibles**
NetFlow	Cisco, Enterasys, Extreme Networks, Foundry Networks, 3com, y Riverbed
sFlow	Alcatel, Extreme Networks, Foundry Networks, Hitachi, NEC, Alaxala

	Networks, Allied Telesis, Hewlett Packard, Comtec Systems, y Force10 Networks
Cflow y J-Flow	Juniper
NetStream	Huawei y H3C
IPFIX	Nortel

Tabla 1: Varios flujos soportados por los proveedores: ***Más información***

Veamos un ejemplo de una solución de software que se basa en el aprovechamiento de los datos contenidos en los flujos para monitorear el ancho de banda de la red de una empresa.

4.Una solución de software basada en flujo

Cuando una empresa global decide utilizar una solución de software basada en flujo para monitorear su empresa global distribuida, el entorno se ve como la siguiente figura. El software se debe implementar en cada una de las ubicaciones remotas y el administrador de la red solo puede ver los datos recopilados de la ubicación en ese nivel o ubicación solamente.

Cuando una empresa global decide utilizar una solución de software basada en flujo para monitorear su empresa global distribuida, el entorno se ve como la siguiente figura. El software se debe implementar en cada una de las ubicaciones remotas y el administrador de la red solo puede ver los datos recopilados de la ubicación en ese nivel o ubicación solamente.

[IMAGEN:

Informes de tráfico · Router 1 · Router 2		
Informes de tráfico · Router 1 · Router 2	Informes de tráfico · Router 1 · Router 2	Informes de tráfico · Router 1 · Router 2

]

Figura 2: Monitoreo típico basado en flujo

El informe sobre el uso del ancho de banda en cada una de las oficinas solo lo puede ver el administrador de red de esa oficina. Aquí, los datos están en silos. Para obtener una vista general consolidada, el administrador de red principal o el CIO deben recopilar los datos disponibles para cada administrador de red.

Desventaja de esta solución

- Falta de una visión unificada:

  Una solución de monitoreo distribuido puede resolver el inconveniente en el modelo anterior. Al recopilar datos de todas las ubicaciones distribuidas y presentarlos en una vista unificada, ofrece un mayor control al administrador de red o al CIO.

5.**Una solución de monitoreo distribuido basada en flujo**

Un ejemplo: NetFlow Analyzer Enterprise Edition

[IMAGEN:

Recopilador remoto	HTTPS	Servidor central	HTTPS	Cliente web (informe y datos)
	HTTPS		HTTPS	
	Recopilador remoto		Recopilador remoto	

]

Figura 3: Monitoreo basado en flujo con recopilación distribuida

NetFlow Analyzer Enterprise Edition es una solución de software escalable basada en flujo de ManageEngine que es ideal para grandes corporaciones con decenas de miles de interfaces. Utiliza recopiladores distribuidos (mostrados en el diagrama anterior), que se instalan en oficinas remotas. Los recopiladores remotos recopilan la información de flujo de todos los routers en la ubicación, procesan y comprimen los datos, y los envían al servidor central a través de un enlace HTTPS seguro. De esta manera, los recursos que se consumen son solo una fracción de lo que se consumiría con otras técnicas de monitoreo de tráfico.

El servidor central recibe los datos comprimidos exportados por todos los recopiladores y los analiza para elaborar informes. El servidor central está idealmente ubicado en la sede principal de la empresa. Un administrador de red principal o CIO puede acceder a los informes generados por el servidor central a través de un cliente web y obtener una vista unificada de toda la red.

NetFlow Analyzer Enterprise Edition:

[IMAGEN:

Es adecuado para grandes empresas con redes distribuidas.	Es escalable para admitir miles de routers y switches.	Ofrece una vista centralizada y unificada para una gestión sencilla.
Utiliza una comunicación segura basada en HTTPS.	Admite términos de servicio (ToS), punto de código de servicios diferenciados (DSCP) e indicadores TCP_Flag.	Admite Cisco NetFlow v5, v7 y v9 junto con sFlow.
No requiere probes de hardware complejos.	Se ejecuta en Windows y Linux, tanto de 32 bits como de 64 bits.	Ofrece precios asequibles a partir de $1.045 por una licencia perpetua.
	Ofrece una evaluación gratis por 30 días sin restricciones en las funciones disponibles.	Incluye soporte receptivo.

]

6. Conclusión

Tenga en cuenta los siguientes puntos clave antes de elegir su solución de análisis de tráfico y monitoreo de ancho de banda para asegurarse de que su inversión ofrece el valor esperado.

9 puntos clave que el CIO o el administrador de red deben tener en cuenta al elegir la solución adecuada

1. Considere qué tipo de solución necesita: Una solución basada en hardware, sondeo, analizador de paquetes o una solución totalmente basada en software.
2. Considere el costo de la solución. Necesita saber cuál será el costo de usar el software durante los próximos cinco años.
    i. Aclare los costos asociados con las actualizaciones de software y el soporte al producto.
    ii. Confirme los costos asociados con la implementación de personal para manejar los desafíos a medida que surgen.
3. Compare la inversión en el producto con el ROI del producto.
    i. Un producto que cuesta más que el ROI que genera nunca es la solución adecuada.
    ii. El monitoreo del ancho de banda es una función destinada a agregar valor a los resultados finales de la empresa. No debería terminar costando al departamento de red más de lo que devuelve en valor.
4. Evalúe el tipo de soporte que ofrece el proveedor.
    i. El número de personal receptivo disponible hace toda la diferencia para usted como cliente. Asegúrese de que su proveedor cuenta con un centro de asistencia con todo el personal y con disponibilidad inmediata.

5. Familiarícese con el legado de la empresa y el producto.
   i. Normalmente, una empresa que ha estado en el negocio durante más de una década y ha logrado seguir siendo rentable es una buena opción.
   ii. Un producto que ha apoyado a miles de clientes en todo el mundo demuestra su sólida capacidad de ingeniería y soporte de primera clase.
6. Elija un proveedor anticipando las necesidades futuras.
   i. No compre una solución teniendo en cuenta solo los requisitos actuales.
   ii. Opte por una empresa que tenga una amplia gama de productos relacionados con la gestión de redes. Además de monitorear todo el ancho de banda de la red empresarial, en el futuro, es posible que desee monitorear el rendimiento de las aplicaciones de la red, analizar los logs del firewall, etc.
   iii. Visualice las necesidades futuras de su red y elija un proveedor que pueda satisfacer esas necesidades.
7. Evalúe a su ritmo.
   Intente extender su licencia de prueba si todavía no está convencido de que sea la solución adecuada. Una empresa que no extiende su licencia o tiene procedimientos engorrosos para hacerlo puede no ser la mejor apuesta en el futuro.
8. Los foros del proveedor pueden ser de gran ayuda.
   Vea qué tan activos e interesantes son los foros. Los foros pueden mostrar lo popular que es el producto y la capacidad de respuesta de los equipos del producto.
9. ¡Por último, no caiga en la trampa de los asesores y los trucos de marketing!

Para obtener más información sobre ManageEngine NetFlow Analyzer, visite manageengine.com/latam/netflow/

Para preguntas técnicas, contacte a: tech-latam@manageengine.com