Primera Conferencia de Directores de Tecnología, TICAL
Gestión de las TI en Ambientes Universitarios, Panamá,20 y 21 de Junio de 2011

Problemas y herramientas en la seguridad de redes de transmisión de datos universitarias. El caso de la Universidad Nacional de Cuyo.

Roberto Cutuli[1] Carlos Catania[2], Carlos García Garino[2,3]

[1] Centro de Información Tecnológico, [2] ITIC, [3] Facultad de Ingeniería
Universidad Nacional de Cuyo, Centro Universitario, 5500 Mendoza, Argentina
rcutuli@uncu.edu.ar, {ccatania, cgarcia@itu.uncu.edu.ar}

Resumen. La infraestructura de red disponible en muchas universidades presenta una serie de inconvenientes afines. Por un lado, como en cualquier otra área se pueden observar altos requerimientos de ancho de banda por parte del personal docente y alumnos. Sin embargo en muchos casos el ancho de banda de los enlaces utilizados está por debajo del nivel requerido. A esta situación se le suma la falta de recursos humanos para tratar con los problemas propios de la administración de una infraestructura de red de gran tamaño como resultan las redes universitarias. Luego, los incidentes producidos por fallas de *hardware*, problemas de configuración y principalmente intrusiones ilegales a la red pueden ocasionar la disminución en el ancho de banda disponible como así también un desgaste innecesario del personal administrativo. Este trabajo presenta un análisis de la situación de la infraestructura de red en la Universidad Nacional de Cuyo y sus mayores inconvenientes. Se discuten además los esfuerzos actuales tendientes al desarrollo de un sistema integrado de asistencia al personal encargado de la administración de la red. La misión de dicho sistema es nuclear los sistemas de administración ya operativos en la red y proveer mecanismos de fusión e integración de información a fin de permitir un control unificado, manteniendo las el nivel de descentralización y autonomía propios de la universidad.

Palabras Clave: Redes de transmisión de datos; seguridad; integración de información

1 Introducción

La administración de una red universitaria es una tarea de alta complejidad que demanda un considerable nivel de conocimiento. Los requerimientos por parte del personal universitario y su comunidad de alumnos son cada vez mayores. Por un lado debe considerarse que el acceso a la información disponible en Internet, constituye un requerimiento fundamental para el diario funcionamiento de cualquier institución de enseñanza, por lo que contar con suficiente ancho de banda es primordial. Por otro lado también existe la necesidad de que los recursos dentro de la infraestructura de red presenten una alta disponibilidad. Actualmente, servicios como el correo electrónico o la mensajería instantánea resultan vitales para la interacción diaria entre los usuarios de la red.

Lamentablemente, en muchos casos las universidades carecen de los recursos suficientes para proveer el ancho de banda adecuado en su infraestructura de red. Otro

inconveniente que se observa con cierta frecuencia es la falta de recursos humanos para la administración de dicha infraestructura. Entonces, es común observar situaciones en las que servicios de red fundamentales se ven afectados por fallas de hardware o problemas de configuración. Sin embargo, el mayor inconveniente lo constituye la imposibilidad de dar una respuesta a tiempo a las posibles violaciones de seguridad. Por otro lado, la falta de recursos humanos, no permite implementar mecanismos que permitan hacer políticas de seguridad adecuadas.

Actualmente existen herramientas (Firewalls, Sistemas de Control de Ancho de Banda, Sistemas de Detección de Intrusos), destinadas a dar soporte al personal encargado de la administración de de la red. Sin embargo, en algunos casos estas no resultan suficientes, debido al alto nivel de descentralización propio de algunas infraestructuras de red dentro del marco académico.

En el presente trabajo se realiza un estudio de la infraestructura de red de la Universidad Nacional de Cuyo (UNCuyo). La UNCuyo es la universidad más grande del centro oeste de Argentina con cerca de 4000 puestos de trabajos y múltiples enlaces hacia otras redes institucionales y la propia Internet. Se discute además los detalles de un sistema que combina los sistemas de administración ya operativos en la red y provee mecanismos de fusión e integración de información a fin de permitir un controlo unificado, manteniendo las el nivel de descentralización y autonomía propios de la universidad.

El trabajo esta organizado de la siguiente manera: en la sección 2 se brinda información institucional sobre la UNCuyo. En la sección 3 se presenta información referida a la infraestructura de red de transmisión de datos su topología y algunas consideraciones respecto a la seguridad. En la sección 4 se discuten las características principales de MIDAS, un sistema orientado a lidiar con los incovenientes propios de la red. Finalmente, en la sección 5 se presentan las conclusiones de este trabajo.

2 La Universidad Nacional de Cuyo

La Universidad Nacional de Cuyo (UNCuyo) [1] se fundó en Mendoza, Argentina en 1939. Actualmente es la casa de estudios superiores más grande del centro oeste argentino. Originalmente sus unidades académicas estaban ubicadas en las provincias de San Luis, San Juan y Mendoza, las cuales conforman la región de Cuyo, de la cual proviene el nombre de la universidad. Desde 1973, año en que se crearon las Universidades Nacionales de San Luis y San Juan, la UNCuyo lleva a cabo su labor en la provincia de Mendoza

Actualmente conforman la Universidad 11 facultades: Artes y Diseño; Ciencias Económicas; Ciencias Médicas, Ciencias Políticas y Sociales; Derecho; Filosofía y Letras; Ingeniería y Odontología, todas emplazadas en el Centro Universitario de Mendoza, ver figuras 1 y 2.

Fig. 1. Foto aérea del campus de la Universidad Nacional de Cuyo. Fuente google maps.

La Facultad de Educación Elemental y Especial se sitúa en el centro de la ciudad a unos 5 km del campus y en la localidad de Chacras de Coria, a 16 km de la ciudad de Mendoza se ubica la Facultad de Ciencias Agrarias. En la ciudad de San Rafael, a 260 km de distancia de Mendoza funciona la Facultad de Ciencias Aplicadas a la Industria. Además de las facultades citadas existen los Institutos de Ciencias Básicas; Tecnológico Universitario, de Seguridad Pública, que funcionan en el ámbito del Gran Mendoza y el Instituto Balseiro sito en la ciudad de Bariloche a unos 1100 km de distancia de Mendoza. La universidad también posee varios colegios secundarios.

Actualmente cursan sus estudios de grado unos 38 mil estudiantes que alcanzan unos 50 mil si se suman los estudiantes de postgrado y los alumnos de los colegios secundarios de la universidad.

La UNCuyo posee una importante valoración social en Mendoza y su zona de influencia que se ha plasmado en el liderazgo y/o participación de diferentes emprendimientos asociativos: la Fundación Escuela de Medicina Nuclear (FUESMEN) pionera en latinoamérica en Medicina por Imágenes; la Fundación del Instituto Tecnológico Universitario (FITU); el Instituto de Desarrollo Industrial, Tecnológico y de Servicios (IDITS) y el Instituto Balseiro en convenio con la Comisión Nacional de Energía Atómica (CONEA), así como relaciones con otras instituciones. Recientemente ha liderado la conformación de la Asociación de Universidades SurAndinas (AUSA) que reúne a distintas casas de estudios cercanas a la cordillera de los Andes.

Fig. 2. Esquema de distribución de las unidades académicas en el campus de la Universidad Nacional de Cuyo.

El cúmulo de relaciones institucionales y académicas, conlleva importante actividad intrainstitucional (que se desarrolla en la distintas unidades académicas sitas dentro o fuera del campus) y extrainstitucional, que en la práctica ha dado lugar a una compleja topología de red de transmisión de datos que se discute en la próxima sección.

3 La red de transmisión de datos. Topología y consideraciones de seguridad

La red de la Universidad Nacional de Cuyo posee unos 4000 puestos de trabajo conectados a la misma. Estos recursos están distribuidos a lo largo de la red que interconecta a las facultades e institutos dentro o fuera del campus Universitario. A estos equipos que hay que adicionarle al menos unos 100 servidores de los cuales la mitad están instalados sobre equipos físicos y los restantes están virtualizados.

3.1 Arquitectura

El esquema de conectividad interno es sencillo ya que se ha trabajado en los últimos años depurando la red para optimizar el funcionamiento e incrementar el rendimiento de acuerdo a la creciente demanda de los servicios que esta provee.

La red interna del campus, que se despliega en la *nube* denominada “Campus Universitario UNCuyo” en el gráfico de la figura 3, se basa en un esquema de interconexión tipo estrella, materializado por un switch. En cada unidad académica se dispone un router que se conecta de manera punto a punto al switch central mediante

enlaces de fibra óptica en la mayoría de los casos. Desde el punto de vista de los protocolos de redes, se emplea IPV4 y se disponen redes privadas en cada unidad académica. Estas redes privadas se rutean dentro del campus. El switch central ya mencionado se conecta a un router central que administra los enlaces hacia el exterior.

Hacia el exterior la red tiene un complejo sistema de interconectividad con el mundo que está fuera del campus universitario al cual se puede acceder, como se observa en el gráfico de la figura 3, por más de un camino o enlace de red.

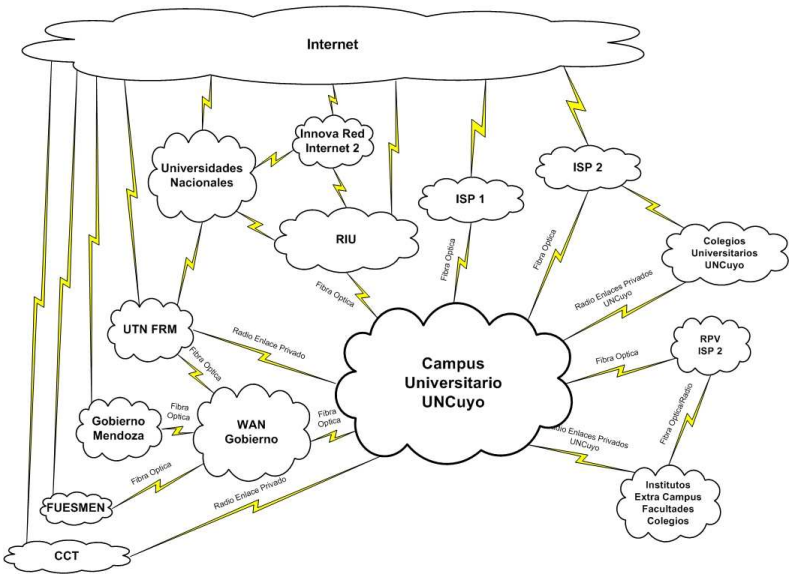

Fig. 3. Esquema de los enlaces de la Red de transmisión de datos de la Universidad Nacional de Cuyo.

Existen varias conexiones a Internet con tecnología de fibra óptica. Mediante las mismas se provee conectividad a Internet 1 por intermedio de distintos ISP y también a Internet 2 a través del enlace a tal efecto provisto a la Red de Interconexión Universitaria (RIU) [2] que se basa en servicios brindados por InnovaRed [3]. RIU también provee a la UNCuyo, así como a las demás Universidades Nacionales servicios de I1 e I2, sobre la cual se ha implementado una red universitaria de telefonía IP.

La red de la UNCuyo también se interconecta por intermedio de la WAN del Gobierno de la Provincia de Mendoza a organizaciones y/o redes externas como la red del Gobierno de la Provincia de Mendoza, la Fundación Escuela de Medicina Nuclear (FUESMEN), la Facultad Regional Mendoza de la Universidad Tecnológica Nacional y otras instituciones conectadas a la WAN.

Además la Red de la UNCuyo se conecta por radioenlaces privados propietarios tipo 802.11 al Centro Científico Tecnológico CCT Mendoza (ex CRICYT) del CONICET, a la Facultad Regional Mendoza de la Universidad Tecnológica Nacional

(configurando un enlace alternativo al citado en el párrafo anterior), y a otras Unidades Académicas y Colegios que están ubicados fuera del campus Universitario, pero dentro del radio del Gran Mendoza.

La facultad de Ciencias Agrarias distante a 16Km del campus Universitario está interconectada mediante un radio enlace privado de la UNCuyo y por medio de la Red Privada Virtual (RPV) de un ISP que brinda además el servicio de Internet. La facultad de Ciencias Aplicadas a la Industria en San Rafael (la más distante del campus a 260km) está conectada por un RPV del mismo proveedor.

En la figura 3 puede observarse además que la mayoría de los colegios y/o institutos que están fuera del Campus Universitario poseen además sus propios enlaces a Internet.

El protocolo de de enrutamiento interior es OSPF [4] y el exterior es BGP [5]. Se dispone de más de 32Mbps de ancho de banda para conexión a Internet, a los cuales hay que añadir otros 50Mbps de conexión hacia redes externas al campus Universitario, distribuidos en varios enlaces con distintas tecnologías de transmisión. Por ejemplo se disponen 10 Mbps con la WAN de Gobierno, 12 Mbps en la Red Privada Virtual para conectar a las Facultades de Ciencias Agrarias y Ciencias Aplicadas a la Industria y 4 radioenlaces de 5 Mbps cada uno de ellos, más otros enlaces menores.

3.2 Análisis de Tráfico

La distribución del tráfico semanal de la red de la UNCuyo se puede observar en la Figura 4. En la misma se puede apreciar el porcentaje de utilización del ancho de banda de la red en función de servicios mayormente utilizados.

Como en la mayoría de las redes actuales el tráfico HTTP y HTTPS ocupan la mayor cantidad del ancho de banda disponible, alcanzando cerca de un 90%. En el caso del tráfico SMTP se observa apenas un 2%. Por otro lado el tráfico de SSH esta cercano al 1.5%. SSH es el protocolo para administración de sistemas basados en el sistema UNIX. El resto corresponde a la suma del tráfico generado protocolos como DNS, proxy e IMAPS.

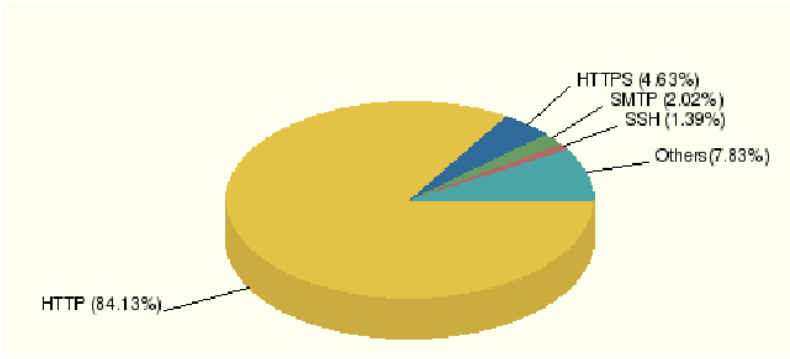

Fig. 4. Distribución del tráfico de la red Universitaria en función de los servicios utilizados

En la figura 5 se presenta la distribución del tráfico de la red de la UNCuyo teniendo en cuenta las direcciones IP origen. Se observa que más del 50% del tráfico saliente es originado por tan solo 10 direcciones IP. Estas direcciones pertenecen su mayoría a los servidores ubicados en las distintas facultades pertenecientes a la Uncuyo. Se observa también entre estas direcciones IP algunos servidores *Proxies* utilizados para tareas de *cache* de datos transferidos hacia la red universitaria.

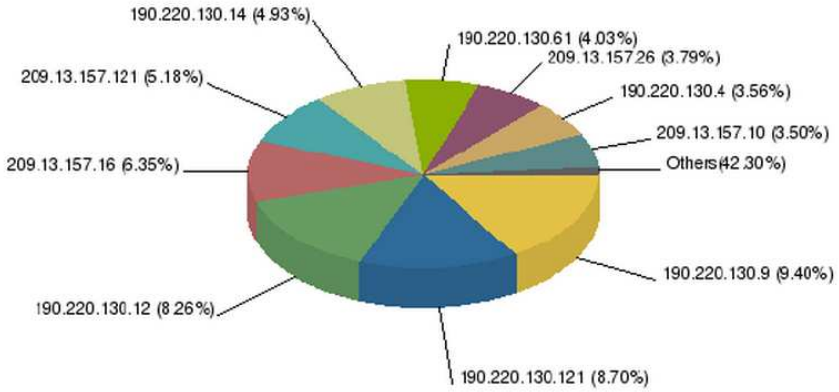

Fig. 5. Distribución del tráfico de la red Universitaria en función de los servicios utilizados

3.3 Situación Actual

Debido a la multiplicidad de enlaces y la complejidad de la red la implementación de un firewall o algún sistema de monitoreo del tipo IDS o IPS en un único punto de la infraestructura no parece adecuado.

Una gran parte de los inconvenientes en el funcionamiento de la red están provocados por los virus que ingresan a la misma. Dado que objetivo de muchos de estos virus el envío de SPAM, se produce una degradación en el servicio de SMTP a causa del tráfico innecesario. Esta situación se ve empeorada por la divulgación de contraseñas por parte de los usuarios internos de la red, lo que provoca un aumento en el envío y recepción de SPAM.

Por otro lado existe un total abuso en el uso de las redes sociales como así también en las aplicaciones P2P que instalan los usuarios. Dadas la variabilidad en las características de las redes P2P resulta difícil lidiar con alternativas para reconocer este tipo de trafico.

La utilización de NAT en muchas de las redes internas hacia Internet, es otro problema usual que se debe resolver, ya que complica la administración e implementación de políticas de uso.

También se observan muchos problemas físicos causados por mal funcionamiento de los dispositivos de red, cableados no estructurados, conexión de Access Points (APs) abiertos a lo largo de toda la red del campus Universitario, servidores de DHCP descontrolados, o sin control alguno, etc.

Cabe señalar que la complejidad que proviene de la multiplicidad de enlaces se incrementa en la práctica por el esquema de gestión que se emplea, que puede denominarse *administración centralizada con delegación de responsabilidades*. En este contexto el Centro de Información Tecnológico (CIT) funciona como una suerte de ISP interno: se reserva la estrategia de gestión global de la red; asigna direcciones IP; monitorea la seguridad e informa de fallas o problemas vinculados a la misma. Por otra parte delega a los administradores de red de las diferentes facultades e institutos actividades como la gestión de sus equipos, configuración de los routers de borde sus redes, etc.

Es importante destacar que actualmente no existe una norma o protocolo de la institucional que recoja la experiencia adquirida y establezca pautas y criterios para el buen funcionamiento de la red. Entonces en la práctica los servicios que se propagan dependen muchas veces de los requerimientos de los administradores de red de las diferentes universidades académicas generando demandas de tráfico a veces difíciles de satisfacer. Con este fin se han dispuesto mecanismos de asignación y control de ancho de banda que regula el acceso de las distintas unidades académicas al ancho de banda disponible.

En el actual contexto de cosas las redes P2P y aplicaciones propias de la Web 2.0 y redes sociales constituyen problemas difíciles de administrar que se espera se incrementen en un futuro cercano, planteando así a mediano plazo escenarios complejos para el acceso a la información.

Con el propósito de mejorar la situación actual y muy especialmente prever dificultades a mediano plazo, se está trabajando en el desarrollo de un sistema integrado de asistencia al personal encargado de la administración de la red. El propósito del mismo es nuclear los sistemas de administración ya operativos en la red y proveer mecanismos de fusión e integración de información a fin de permitir un control unificado, manteniendo el nivel de descentralización y autonomía propios de la universidad.

4 Automatización en el proceso de gestión de la red mediante MIDAS

MIDAS (autonoMous Intrusion Detection Assistance System) es un sistema orientado a brindar soporte al administrador de red en las tareas de reconocimiento de anomalías y comportamientos maliciosos dentro de la infraestructura de red.

MIDAS aborda el problema de gestión de la red desde dos puntos de vista. En primer lugar, el objetivo de MIDAS es disminuir la necesidad de interacción humana en el proceso de gestión y reconocimiento de amenazas en el tráfico de red. En segundo lugar, en aquellas situaciones donde la seguridad del personal de seguridad no se pueda evitar, MIDAS proporciona información resumida referente a los incidentes de seguridad. La información de resumen se presenta en forma de reglas

que describen los incidentes seguridad detectados, evitando de esta manera la necesidad de analizar el conjunto de registros de tráfico perteneciente al incidente de seguridad detectado y facilitando así el ajuste del sistema.

Una de las ventajas principales de MIDAS es su capacidad para interactuar con los sistemas de análisis de tráfico y sistemas de detección presentes en la red. MIDAS recopila la información desde diferentes fuentes y la procesa mediante diversas técnicas de clasificación y fusión de información. A partir de los resultados MIDAS es capaz de reconocer anomalías en el tráfico de la red, como así también intrusiones.

MIDAS cuenta con un mecanismo de detección de anomalías basado en técnicas estadísticas y de aprendizaje automático [6]. El modelo de tráfico normal generado de manera automática, permite reconocer problemas comunes de la red como violaciones de políticas de uso o servicios configurados de manera errónea. Otra de las ventajas es la posibilidad de reconocer intentos de intrusiones que hagan uso vulnerabilidades aun no conocidas.

4.2 Arquitectura

En términos generales en la arquitectura de MIDAS se pueden observar cuatro módulos:

Módulo de adquisición de tráfico: encargado de la recolección del tráfico de la red en crudo. La adquisición del tráfico se realiza de manera descentralizada, mediante la colocación de sensores distribuidos estratégicamente a lo largo de la infraestructura de red. La información adquirida es luego enviada a un repositorio central para su posterior análisis. De esta manera, se puede manejar el alto grado de centralización observado en la infraestructura universitaria.

Módulo de extracción de atributos de tráfico: a partir del tráfico obtenido se extrae un conjunto de atributos relevantes para el proceso de análisis y detección de anomalías.

Modulo de detección de incidentes: procesa las instancias de tráfico obtenidas por el modulo de extracción de atributos de tráfico. En este módulo se determina si una instancia de tráfico dada corresponde a un incidente de seguridad o una violación de las políticas universitarias establecidas. En este módulo se combinan las distintas herramientas de análisis de incidentes y detección de anomalías utilizadas en la infraestructura de red.

Modulo de administración: se encarga de presentar información sobre los incidentes observados en la red. Una de las principales características de este módulo es la capacidad de resumir la información obtenida de forma inteligente mediante la aplicación de técnicas de computación evolutiva.

4.2 Modos de operacion.

MIDAS pose tres modos de operación diferentes: estado estacionario (véase la figura 6), generación inicial de los modelos de tráfico (Véase la figura 7) y el ajuste periódico en los modelos de tráfico (véase figura 8).

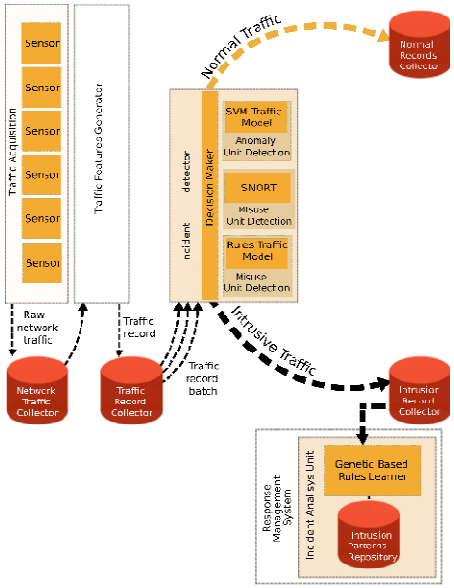

Fig. 6. MIDAS: Flujo operacional durante el proceso de análisis y reconocimiento de anomalías en el tráfico de la red.

La figura 6 muestra el flujo de datos durante la etapa de generación inicial del modelo. En este caso, sólo las herramientas de detección y análisis de tráfico están operativas. Por lo tanto, al principio, el modulo de detección de incidentes evaluará las instancias de tráfico únicamente en función de los resultados de herramientas como FORTIGATE [7] o SNORT [8]. Aquellas instancias de tráfico consideradas sospechosas como así también aquellas consideradas normales son almacenadas en sus respectivos repositorios por un periodo determinado de tiempo. Luego de transcurrido ese periodo, las instancias de tráfico normal son utilizadas para la construcción de un modelo de normalidad del trafico de red. Por otro lado, las instancias de tráfico reconocidas como sospechosas se utilizan para la generación de reglas de clasificación por medio de técnicas de computación evolutiva. Dichas reglas se almacenan en un repositorio de reglas que forma parte de la *Unidad de Análisis* del módulo de Administración, para su posterior evaluación por parte del personal de seguridad

A partir de este punto, MIDAS comienza con su funcionamiento normal (modo estacionario) en donde la detección de incidentes se realiza de acuerdo a opiniones recogidas de los diferentes mecanismos de detección como se observa en la figura 7.

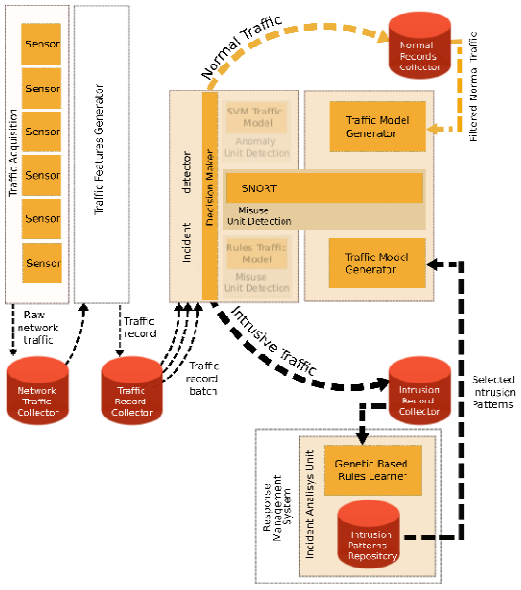

Fig. 7. MIDAS: Flujo operacional durante el proceso de generación de los modelos de tráficos

Periódicamente, MIDAS comienza con su mecanismo de ajuste de forma automática. Como se puede observar en la figura 8. Durante este periodo, las reglas de clasificación se actualizan de acuerdo a las nuevas instancias de tráfico consideradas sospechosa, las cuales fueron almacenadas en el correspondiente repositorio. Por otro lado las nuevas instancias de tráfico normal se utilizan para realizar la actualización del modelo de normalidad del tráfico. Sin embargo en este caso, las instancias de tráfico normal han sido preprocesadas por los diferentes mecanismos presentes en el modulo de detección de incidentes. Además, el personal de seguridad tiene la oportunidad de analizar el contenido del repositorio de reglas en el interior del módulo la administración, y determinar si las reglas obtenidas describen comportamiento *intrusivo* o *anómalo* válido. Luego, un subconjunto de dichas reglas pueden ser agregada al mecanismo de detección basados en reglas mencionado anteriormente.

5 Conclusiones

La Red de transmisión de datos de la Universidad Nacional de Cuyo presenta algunas características generales que se comparten con otras universidades argentinas: gran demanda de ancho de banda; tráfico de protocolo P2P, uso cada vez mayor de redes sociales así como algunas características propias: un trabajo valioso de ingeniería de la red del campus y un esquema complejo de enlaces hacia el exterior

del mismo, algunos dedicados a Internet, uno dedicado a I2 y otros enlaces dedicados de la universidad o bien para interconexión con otras instituciones.

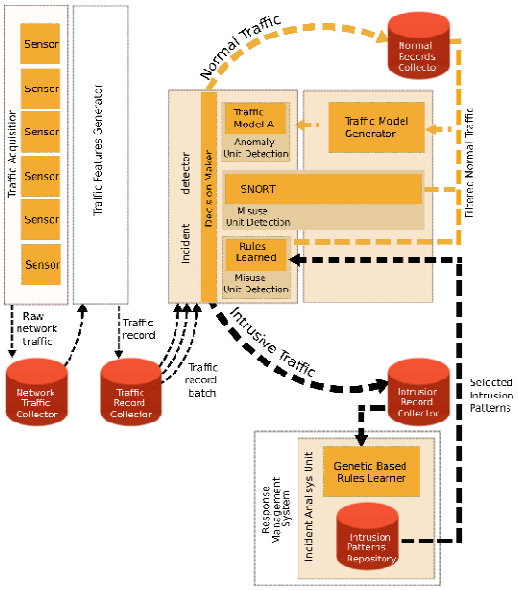

Fig. 8. MIDAS: flujo de operaciones durante el proceso de ajuste periódico de los modelos

Actualmente no se dispone de protocolos institucionales que brinden normas y pautas de uso para las redes de transmisión de datos en la UNCuyo, problema que en el contexto de la presente conferencia TICAL bien puede enmarcarse en el contexto de gobernabilidad de las TICs. Es interesante destacar el esquema de gestión denominado administración centralizado con delegación de responsabilidades, que en la práctica requiere de un fuerte compromiso por parte de los administradores de facultades o institutos.

La complejidad de los enlaces hacia el exterior, ya sea los destinados a internet o a otros fines, que plantean una topología con múltiples puntos de acceso, vuelven compleja la administración de la seguridad, aspecto que en ocasiones puede potenciarse si no existe una fuerte coordinación entre los administradores de red del campus y las facultades e institutos.

En el actual contexto de situación se han dispuesto equipos específicos para ayudar en la administración como controladores de ancho de banda; el analizador FORTINET o bien elementos más tradicionales como Firewalls y Proxys. También se monitorean los enlaces mediante herramientas como MRTG que relevan el tráfico de servidores y routers mediante el protocolo SMNP. Mediante una fuerte carga de trabajo sobre recursos humanos a nivel administradores de red y las herramientas

señaladas se ha controlado el número de incidentes de seguridad y se puede brindar una aceptable respuesta frente a incidentes de seguridad ocurridos.

A mediano plazo la situación tenderá a agravarse porque se espera mayor competencia interna por el ancho de banda, un elemento siempre escaso, una mayor participación de herramientas de redes sociales y web 2.0 que pueden tornar insuficientes las medidas dispuestas en la actualidad.

La implementación de sistemas de administración de seguridad como MIDAS, que permite controlar en forma distribuida múltiples puntos de acceso, la posibilidad de contar con una base de datos del tipo de tráfico habitual, caracterizado mediante reglas adecuadas, brinda la posibilidad de mejorar la situación actual y, muy especialmente, contemplar los potenciales problemas previstos a mediano plazo.

Desde un punto de vista más general cabe señalar que el trabajo conjunto de profesionales a cargo de la operación de la red universitaria (CIT) con un equipo de gente dedicado al desarrollo (ITIC) plantea un escenario promisorio de beneficio mutuo y complementario entre ambos equipos de trabajo y potenciales ventajas para la universidad. Puede decirse que se verifica en la práctica que esquemas de cooperación, en este caso intrainstitucionales, conducen a mejoras valiosas, como se señala en los manuales de gestión y cooperación científica y tecnológica.

Agradecimientos

Los autores agradecen a la Agencia Nacional de Promoción Científica y Tecnológica (ANPCyT) la financiación parcial brindada a través del l Proyecto PAE-PICT 3279.

Referencias

1. Reseña Histórica de la UNCuyo: http://www.uncu.edu.ar/paginas/index/resena-historica.
2. Red de Interconexión Universitaria Argentina: www.riu.edu.ar.
3. InnovaRed, Red Nacional de Educación e Investigación en Argentina: www.innova-red.net.
4. Rekther, Watson, Li *A Border Gateway Protocol*, RFC 1771, 1995
5. Moy *Open Shortest Path First Protocol Versión 2* RFC 2178, 1998
6. Catania, C.; Bromberg, F. & Garcia Garino, C. Bromberg, F. & Verdun, L. (Eds.) *An autonomous labeling approach to SVM algorithms for network traffic anomaly detection* Proceedings of ASAI 2009 Argentine Symposium on Artificial Intelligence, 2009, 144-158
7. FORTINET, www.fortiwall.com/fortigate-310b.html
8. Roesch, M. SNORT - Lightweight Intrusion Detection for Networks Proceedings of the 13th USENIX conference on System administration, USENIX Association, 1999, 229-238