https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 108 - 121

Comunicación IPv4 segura entre áreas universitarias a través de conexiones de Internet

Información del reporte:

Para citar este reporte técnico:

Martínez Quinto, M. (2025). Comunicación IPv4 segura entre áreas universitarias a través de conexiones de Internet. *Cuadernos Técnicos Universitarios de la DGTIC, 3* (3) páginas(108 - 121).

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125

Marcial Martínez Quinto
Dirección General de Cómputo y de Tecnologías de Información y Comunicación
Universidad Nacional Autónoma de México
mmarcial@unam.mx
ORCID: 0009-0006-0242-8897

Resumen

Las áreas universitarias cuentan con el acceso a Internet y a RedUNAM a través de enlaces contratados a proveedores de servicios de Internet. Este esquema de red ofrece la conexión directa al campus de Ciudad Universitaria con enlaces dedicados privados (*LAN-to-LAN* y de red privada virtual empresarial). Sin embargo, al presentarse una falla en esas conexiones directas, la comunicación de las áreas universitarias se ve interrumpida, ya que se pierde el servicio de DNS y de recursos de RedUNAM, por lo que la afectación en algunos sitios es prácticamente total. La mitigación del impacto de esos incidentes se realiza de manera manual con la intervención del personal de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación a través del área responsable de velar por la continuidad de la comunicación hacia y desde las áreas universitarias foráneas a Ciudad Universitaria. La necesidad de tener un esquema de red automatizado, para que dicha mitigación no sea manual y se pierdan valiosos minutos en el restablecimiento de la comunicación, dio como origen la elaboración de una alternativa de conexión con los mismos recursos de operación actuales, de forma que, a pesar de que se presenten fallas en cualquier hora del día, los cambios automáticos del tráfico no sean percibidos por los usuarios. Una VPN, construida sobre los enlaces de Internet que brinde seguridad a la información intercambiada, es la solución propuesta en este reporte técnico.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 109 - 121

Palabras clave:

Seguridad, túneles, GRE, IPSec, enlaces a Internet.

Abstract

University campi have access to the Internet and RedUNAM through links contracted with Internet service providers. This network scheme offers direct connection to the Ciudad Universitaria campus with dedicated private links (LAN-to-LAN and enterprise virtual private network). However, if these direct connections fail, communication between university campi is interrupted, as DNS service and RedUNAM resources are lost, resulting in almost complete outage in some locations. The impact of these incidents is mitigated manually with the intervention of staff from the General Directorate of Computing and Information and Communication Technologies, through the area responsible for ensuring the continuity of communication to and from university campi outside Ciudad Universitaria. The need for an automated network scheme to avoid manual mitigation, which would waste valuable time restoring communication, led to the development of an alternative connection using the same current operating resources. This would ensure that, even if failures occur at any time of day, users would not notice the automatic traffic changes. A VPN built over Internet links that provides security for the information exchanged is the solution proposed in this technical report.

Keywords:

Security, tunnels, GRE, IPSec, Internet links.

1. INTRODUCCIÓN

De acuerdo con el manual de organización de la Dirección General de Cómputo de Tecnologías de Información y Comunicación (DGTIC) (Universidad Nacional Autónoma de México [UNAM], 2024), dos de las funciones del Departamento de Monitoreo de DGTIC (NOC RedUNAM) son: monitorear la operación de la infraestructura de conexión de RedUNAM y vigilar su funcionamiento dentro del marco técnico de los contratos correspondientes, en las áreas universitarias de la Zona Metropolitana y del interior de la república (p. 65).

Las conexiones que sirven para comunicar a las áreas universitarias foráneas al Campus Ciudad Universitaria (CU) con la RedUNAM en Ciudad Universitaria son enlaces privados de uso exclusivo para la entidad o dependencia. Estos últimos pueden ser *LAN-to-LAN* o un servicio de red privada virtual empresarial con infraestructura compartida de forma segura sin que el tráfico de cada cliente se vea entre sí. También hay enlaces de Internet que están destinados para acceder a ese recurso, ya sea con fin comercial o para llegar a contenido académico de otras instituciones de educación e investigación. Como lo menciona Tanenbaum (2011), este tipo de conexiones son llamadas WAN (*Wide Area Network*), debido a que interconectan nodos situados en distancias largas, comúnmente a nivel regional, dentro de un país o incluso a través de continentes (p. 23); además, son contratadas a través de los procesos de adquisición o de renta de servicios con base en la legislación universitaria vigente.

El esquema de comunicación en la WAN de RedUNAM de las áreas universitarias foráneas al Campus CU tiene el principal reto de que, al fallar el enlace *LAN-to-LAN* o de red privada virtual que conecta a RedUNAM, se pierde el acceso al servicio de DNS y a los propios recursos de la Universidad. Si bien se

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 110 - 121

puede hacer el enrutamiento del tráfico a través de las conexiones de Internet para que así recobren su conectividad a RedUNAM en Campus CU, no es de forma automatizada, por lo que se pierde valioso tiempo mientras se hace ese cambio manualmente, sin mencionar que el tráfico queda expuesto a las vulnerabilidades existentes en Internet.

En lo que respecta a la comunicación a Internet, debido a que la UNAM cuenta con su propio direccionamiento en las áreas universitarias donde hay enlaces gestionados por el NOC RedUNAM, el intercambio de información con el proveedor de servicios de Internet (ISP por sus siglas en inglés), se hace a través del protocolo BGP con las redes locales (LAN por sus siglas en inglés) de longitud de prefijo de 24 bits para IPv4, mientras que el tráfico de las redes locales con longitud de prefijo mayor (que significa una menor cantidad de nodos disponibles por subred), transita por los enlaces de conexión a RedUNAM al Campus CU (LAN-to-LAN y de red privada virtual empresarial). Por convención entre las organizaciones de Internet, la longitud de prefijo de 24 bits para IPv4 es la más pequeña para propagarse a través de los ISP (Amazon, s.f.), con lo que se busca cumplir las recomendaciones del Grupo de Trabajo de Ingeniería de Internet (IETF por sus siglas en inglés) para obtener el beneficio de una tabla de enrutamiento reducida de redes publicadas en Internet (IETF, 1993).

En el NOC RedUNAM, desde 2022, se ha buscado brindar una alternativa de comunicación automatizada con los recursos actualmente en operación, como lo son los enlaces de Internet que ya están en servicio en las áreas universitarias, de las cuales el personal de DGTIC gestiona su infraestructura y funcionamiento. Así, en escenarios de incidentes de falla de los enlaces de Internet contratados por la UNAM, cuando al menos uno de ellos esté operando, se aprovecha el mayor ancho de banda que hay en esas conexiones y la infraestructura de red de la que se dispone.

2. METODOLOGÍA

La infraestructura actual, que soporta las conexiones WAN de RedUNAM, es, en su gran mayoría, Cisco, por lo que el diseño se basó en los sistemas operativos de este fabricante. Asimismo, el protocolo de enrutamiento interno (IGP por sus siglas en inglés) en RedUNAM es OSPF, por lo que también se consideró en el diseño.

Mediante la *suite* o conjunto de protocolos de IPSec (*Internet Protocol Security*), se puede establecer una conexión segura a través de la red pública de Internet, cifrando el tráfico para evitar que pueda ser visto por terceros que no son los destinatarios del mensaje que se quiere transmitir. Gracias a que es un estándar, tal como lo apunta Aparicio-Izurieta (2022), es soportado por la mayoría de los fabricantes, brindando autenticación, confidencialidad e integridad de la información (pp. 981-982), por lo que se consideró como parte de la solución de VPN implementada.

Un túnel GRE (*Generic Routing Encapsulation*) funge como vía de comunicación virtual entre dos dispositivos que soporten la encapsulación. Así, el mensaje IP original es encapsulado dentro de un paquete GRE, que a su vez es encapsulado en otro paquete IP para su enrutamiento (IETF, 1994a). De esta manera, el mensaje original está dentro de otro paquete IP que tiene el direccionamiento enrutable en Internet, de forma que la conexión entre los dos extremos simula ser directa, mientras la red de en medio sirve de transporte o tránsito. En la solución de VPN propuesta e implementada, la red de tránsito es Internet.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 111 - 121

La solución propuesta es el establecimiento de una red privada virtual (VPN por sus siglas en inglés) que consiste en una conexión de punto a punto; ésta simula una conexión directa entre los dos nodos que se comunican, pero funciona sobre un túnel GRE construido sobre una red de TCP/IP, que, en este caso, es la red de Internet. De acuerdo con De Almeida (2024), IPSec es el estándar de seguridad con la estructura más completa usado en VPN, por lo que, con ese conjunto de protocolos, se asegura que los mensajes serán conocidos sólo por los dispositivos que lo tengan habilitado con los parámetros previamente acordados (p. 4).

Adicional a lo anterior, con la configuración de una traducción de direcciones de red (NAT por sus siglas en inglés), se logra que el tráfico de todas las LAN de las áreas universitarias salgan a Internet y a RedUNAM, utilizando las direcciones IP de los ISP con las que son enumerados los enlaces de Internet y que son conocidas globalmente (IETF, 1994b). De esta forma, se supera la limitante por la convención de proveedores de Internet para que las redes locales con máscara mayor a 24 bits no se vean afectadas por las fallas de los enlaces a RedUNAM (LAN-to-LAN y red privada virtual empresarial).

2.1 DISEÑO

El diseño se hizo primero sobre una maqueta elaborada con el software GNS3 que permite emular los sistemas operativos de los *routers* Cisco, con lo que se evitó hacer pruebas desde cero en equipos en producción. La maqueta puede realizarse con los sistemas operativos soportados por defecto, como los modelos 7200 y dispositivos servidores o computadoras personales que forman parte del propio GNS3 para hacer las pruebas necesarias, tal como lo menciona Salman (2017) en sus pruebas con esa herramienta (p.857).

2.2 CONFIGURACIÓN

Para hacer la configuración, primero se elaboraron los *scripts* en un archivo de texto plano (TXT) antes de aplicarlos a los equipos *routers*.

Para configurar IPSec, es preciso determinar si operará en modo transporte o en modo túnel. Como nos recuerda De Almeida (2024), la diferencia es que el modo transporte se utiliza ampliamente en estructuras donde ya hay implementación de IPSec previa. En cambio, el modo túnel es empleado grandemente en estructuras donde no se ha implementado IPSec, tal es el caso de Internet (Andreoli, 2008, como se citó en De Almeida, 2024, pp. 6-7). Técnicamente, el mensaje original es cifrado en su totalidad en modo túnel, incluido el direccionamiento IP, mientras que, en modo transporte, sólo es la parte del mensaje que corresponde a la información que desea comunicarse. En el caso de la solución propuesta, como lo menciona Aparicio-Izurieta (2022), se usó el modo túnel, que es el método de operación más común cuando se utilizan *routers* que se encargan de procesar el tráfico con IPSec, quedando los equipos de las redes locales y sus aplicaciones sin la necesidad de implementar seguridad (p. 985). Esta forma de implementación de una VPN con IPSec es llamada *Site-to-Site*.

De acuerdo con las recomendaciones de Hadood (2024), el siguiente procedimiento es una buena práctica para establecer una VPN *Site-to-Site* en equipos Cisco:

Definir las credenciales ISAKMP para el intercambio de llaves.

Definir las credenciales de IPSec para el intercambio de datos o información.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 112 - 121

Definir el tráfico de interés para el cifrado a través de una *access-list*.

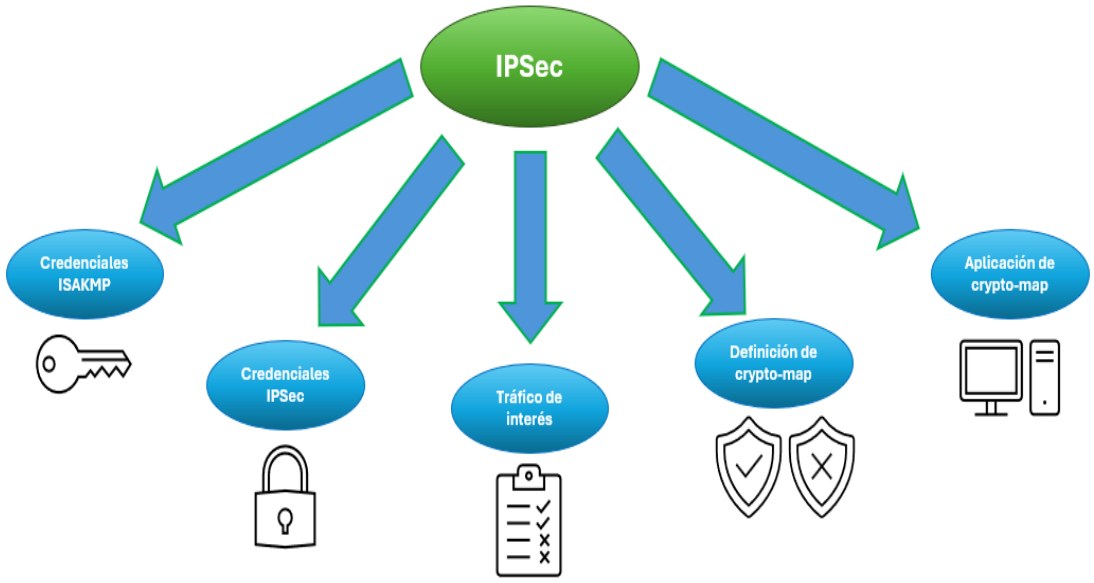
Hacer el *mapping* de todas las credenciales de la VPN en un *crypto map*.

Aplicar el *crypto map* a una interfaz (p. 2305).

Gráficamente, se pueden ver, en la Figura 1, los elementos utilizados para establecer IPSec en la solución propuesta.

Figura 1

Elementos para la implementación de IPSec



El procedimiento que se siguió para la implementación de la VPN con IPSec y túneles GRE se puede examinar con detenimiento en el Anexo A de este documento.

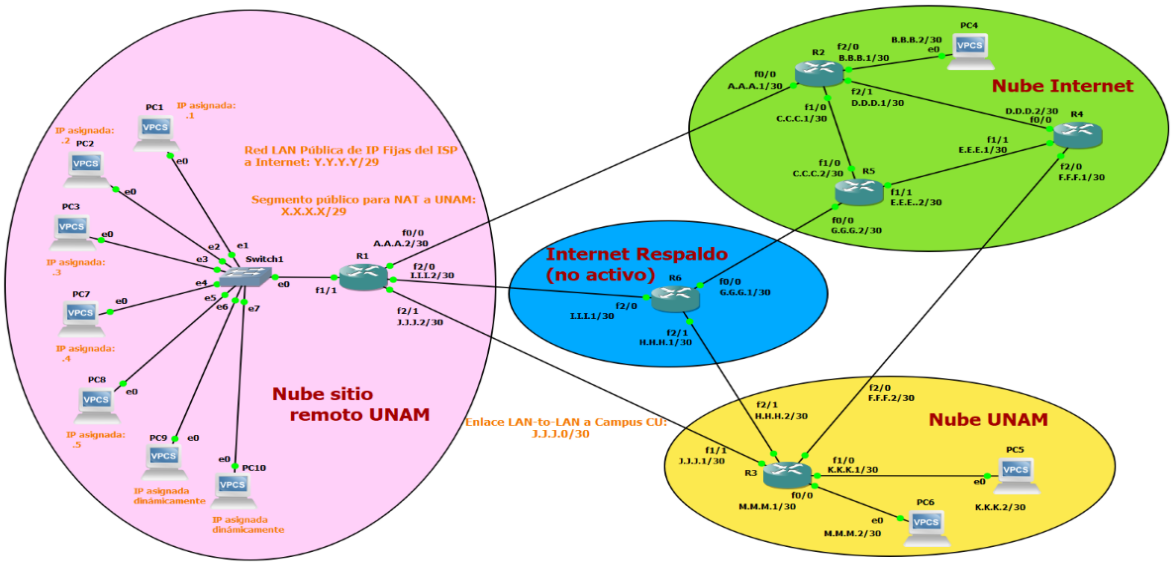
2.3 PRUEBAS

Las pruebas se llevaron a cabo primeramente en una maqueta elaborada en la herramienta de software GNS3, siendo ésta la opción ideal, considerando que fue el primer intento en revisar la factibilidad de la infraestructura actual de RedUNAM en este nuevo paradigma de comunicación. En la Figura 2 se puede apreciar la topología utilizada.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 Vol. 3, Núm. 3. julio-septiembre 2025, págs. 113 - 121

Figura 2

Topología de la maqueta utilizada para las pruebas de la VPN (túneles GRE + IPSec) en la herramienta GNS3



Nota. Por confidencialidad, el direccionamiento IP empleado fue cambiado, pero puede sustituirse por cualquier otro para su adaptación en entornos diferentes. En esta figura, la parte correspondiente al Internet Respaldo tiene la acotación "(no activo)", ya que no siempre hay dos enlaces de Internet en los sitios UNAM; dependerá si aplica esta segunda conexión en cada área universitaria.

Las pruebas en la maqueta constaron de la validación de conectividad entre el sitio remoto y el sitio central, pasando a través de las conexiones de Internet disponibles en dicho sitio remoto. Las verificaciones se llevaron a cabo con las utilidades *traceroute* para corroborar que las trayectorias del tráfico eran correctas (sobre todo si hay dos conexiones de Internet y una de ellas se considera la principal) y *ping* para comprobar que sí había respuesta de los equipos con los que se hizo la comunicación de punta a punta (con una respuesta exitosa de *ping*).

Una vez que se obtuvieron los resultados de comunicación IP satisfactorios, el siguiente paso fue implementarlos en escenarios en producción, con los riesgos que esto conlleva, ya que, si bien hubo resultados correctos a nivel IP, la prueba contundente siempre es a nivel de aplicación.

2.4 IMPLEMENTACIÓN

Con las pruebas satisfactorias en software, lo consecuente fue determinar los sitios para cubrir las áreas universitarias que tienen los diferentes tipos de enlaces contratados para conectarse a RedUNAM. Los nodos seleccionados por cumplir con los requisitos necesarios para su implementación y por la disposición para participar por parte de sus responsables de red fueron los siguientes:

- Un plantel de nivel bachillerato en CDMX que tiene un enlace *LAN-to-LAN* y un enlace de Internet,

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 114 - 121

además de redes locales con máscara igual y mayor a 24 bits.

- Una sede de investigación en el interior de la república que tiene un enlace de red privada virtual empresarial y un enlace de Internet, además de una red local de máscara de 24 bits y con el servicio de telefonía institucional.
- Una facultad en la Zona Metropolitana de CDMX que tiene un enlace *LAN-to-LAN* y un enlace de Internet, además de redes locales con máscara igual y mayor a 24 bits.

Las pruebas de concepto se desarrollaron con la solicitud previa y posterior a la confirmación de los responsables de red de las áreas universitarias involucradas, para que, en caso de una afectación sensible, se contara con un espacio de tiempo que permitiera regresar al estado de operación anterior a la ejecución del cambio. Siempre hubo retroalimentación directa con los responsables de red de esas áreas universitarias, verificando su acceso a las aplicaciones de RedUNAM e Internet.

3. RESULTADOS

En los tres sitios fue satisfactoria la implementación, obteniendo la comunicación correcta a Internet, mientras que la comunicación a RedUNAM se logró que fuera mediante de la VPN construida sobre sus enlaces de Internet y utilizando los túneles GRE protegidos con IPSec.

Con pruebas de utilidades como trazados de ruta y pings, así como con las pruebas de aplicaciones validadas por los responsables de red y sus usuarios, como lo son vía web y aplicaciones móviles y de computadora de escritorio, se pudo confirmar el correcto acceso a Internet a través del NAT (redes LAN con máscaras de red mayores a 24 bits) o directamente (redes LAN con máscaras de red de 24 bits), mientras que, a RedUNAM, fue mediante la VPN-UNAM de túneles GRE con IPSec (para todas las redes LAN). Para lograrlo, se cambió el tamaño del paquete IP, evitando la fragmentación; este punto se aborda mejor en el Anexo A.

Sin embargo, se encontraron fallas que contribuyeron a la mejora de la atención de incidentes que se presentan en RedUNAM. El primer error fue que, debido al NAT, al enmascarar las IP UNAM originales, ya no pueden ser accedidas desde Internet, como con una conexión remota de SSH. La respuesta es retirar de las reglas del NAT, puntualmente de las listas de acceso, las IP específicas que deben ser vistas con IP UNAM desde Internet. Adicionalmente, con el NAT, pueden requerirse muchas traducciones de IP para enmascarar el tráfico, por lo que, al llegar a un límite que depende del *router*, su licenciamiento y hardware, pueden presentarse fallas en el acceso a Internet de las redes locales con máscara mayor a 24 bits. Para resolver este problema, es necesario configurar el NAT en modo de *Carrier Grade*, es decir, darle al proceso del NAT más memoria, retirando información que no es indispensable para su funcionamiento, tal como lo recomienda el fabricante (Cisco, 2016).

Otro problema fue que, cuando hay una falla en los enlaces LAN-to-LAN e Internet, se pueden presentar *loops* que impiden que se logre la comunicación entre las áreas universitarias y el Campus CU, debido a que se genera un comportamiento inesperado con el protocolo OSPF. Esto se corrige reiniciando el proceso de OSPF en los *routers* de los sitios remotos.

Estas problemáticas ya fueron incorporadas al procedimiento para la atención de incidentes de la VPN-UNAM (túneles GRE con IPSec), que sirve para resolver fallas en ese esquema de conexión a RedUNAM.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 115 - 121

Otro hallazgo de gran importancia es que se identificó la necesidad de licenciamiento para que el equipo *router* haga el cifrado del tráfico, de acuerdo con el *throughput* soportado por el dispositivo y con el ancho de banda utilizado sólo para la VPN. Esta consideración depende de cada fabricante y de su línea de licencias para ese propósito. En los tres sitios, se pudo hacer la implementación en un período de licencia que, si bien no tiene soporte de mantenimiento y tiene una limitación en la cantidad de tráfico a cifrar, operativamente sí está permitida por los *routers*, por lo que se pudo continuar la implementación sin inconvenientes.

Cobró mayor importancia tener un esquema de configuraciones de seguridad que permitiera agregar una capa adicional para proteger tanto a los equipos de red, como al tráfico. Un ejemplo lo fue la plantilla de configuración del NOC RedUNAM, que cuenta con líneas para restringir el acceso al dispositivo de enrutamiento (*router*, *switch* o *firewall*), así como la adopción de buenas prácticas de enrutamiento, como lo es la iniciativa MANRS de la Sociedad de Internet (ISOC por sus siglas en inglés). De esta manera, no sólo hay protección en el tráfico, sino también en los equipos de red.

4. CONCLUSIONES

Es claro que, al tener una variedad de enlaces para conectar las áreas universitarias foráneas a RedUNAM, hay ventajas y desventajas, pero el inconveniente principal es que, al quedar fuera la conexión directa al Campus CU, una falla de este tipo puede resultar catastrófica al ocasionar la intervención manual para el restablecimiento de la comunicación.

La VPN mediante túneles GRE con IPSec representa la respuesta automatizada para que, en caso de incidentes en los enlaces WAN, se mantenga el acceso a RedUNAM en las áreas universitarias que se ven afectadas por la falla de sus enlaces. Incluso, se puede prescindir de las conexiones directas al Campus CU que resultan de alto costo, ya que basta con tener enlaces de Internet para poder construir la VPN-UNAM y así establecer la comunicación de forma segura.

Es de resaltar que se debe considerar el hecho de contratar los enlaces de Internet a distintos proveedores, ya que eso incrementa la probabilidad de mantener el acceso a RedUNAM e Internet, en caso de que algún ISP presente fallas en su red e incluso si entra en un estado de contingencia.

Finalmente, pero no menos importante, el equipo técnico responsable de la atención de incidentes de la VPN debe actualizar sus procedimientos para reducir al máximo las afectaciones por fallas y las soluciones de los problemas que se lleguen a presentar en esta nueva forma de conexión a RedUNAM e Internet.

AGRADECIMIENTOS

Tomo este espacio para agradecer a mi jefe, Hugo Rivera, jefe del Departamento de Monitoreo de DGTIC, por darme la confianza de elaborar esta propuesta y por considerarla para los próximos procesos de adquisición de servicios WAN, ya que, a través de esa oportunidad, siento que he aportado y retribuido a mi Universidad.

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 116 - 121

REFERENCIAS

Amazon Web Services Inc. (s.f.). Requirements and quotas. *Why is a /24 the smallest IP range that can be used with BYOIP?* https://repost.aws/articles/ARiVYfeM1dS4STKKhkf7LA_Q/why-is-a-24-the-smallest-ip-range-that-can-be-used-with-byoip

Aparicio-Izurieta, V. V. (2022). Segurança IP segura na Internet (IPSEC). *Sapienza: International Journal of Interdisciplinary Studies, 3(1),* 978–987. https://doi.org/10.51798/sijis.v3i1.278

Cisco Systems Inc. (2016, abril). *IP Addressing: NAT Configuration Guide*. Recuperado el 9 de abril de 2025 de https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-16/nat-xe-16-book/iadnat-cgn.html

Cisco Systems Inc. (2020, octubre). *Next Generation Cryptography*. Recuperado el 8 de abril de 2025 https://sec.cloudapps.cisco.com/security/center/resources/next_generation_cryptography

Cisco Systems Inc. (2023, mayo). *Resolve IPv4 Fragmentation, MTU, MSS, and PMTUD Issues with GRE and IPsec*. Recuperado el 9 de abril de 2025 de https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html

Cisco Systems Inc. (2024, abril). *Understand IPsec IKEv1 Protocol*. Recuperado el 8 de abril de 2025 de https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/217432-understand-ipsec-ikev1-protocol.html

Hadood, A. K. M. (2024). Implementation of Site to Site IPsec VPN Tunnel using GNS3 Simulation. *International Journal for Research in Applied Science & Engineering Technology (IJRASET),* 12(11), 2302–2307. https://doi.org/10.22214/ijraset.2024.65635

Internet Engineering Task Force. (IETF, septiembre 1993). *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*. https://www.rfc-editor.org/rfc/rfc1519.html#page-9

Internet Engineering Task Force. (IETF, octubre 1994a). *Generic Routing Encapsulation (GRE)*. https://www.rfc-editor.org/rfc/rfc1701.html

Internet Engineering Task Force. (IETF, mayo 1994b). *The IP Network Address Translator (NAT)*. https://www.rfc-editor.org/rfc/rfc1631.html#page-2

De Almeida, F. M. (2024). *O universo das ciências exatas e da terra: teoria e aplicações 2*. Brasil: Atena Editora.

Salman, F. A. (2017). Implementation of IPsec-VPN Tunneling using GNS3. *Indonesian Journal of Electrical Engineering and Computer Science),* 7(3), 855–860. https://doi.org/10.11591/ijeecs.v7.i3.pp855-860

Tanenbaum, A. S. (2011). *Computer Networks*. Estados Unidos de América: Pearson Education.

The National Cyber Security Centre of United Kingdom (2022, marzo). *Using IPsec to protect data*. https://www.ncsc.gov.uk/pdfs/guidance/using-ipsec-protect-data.pdf

Universidad Nacional Autónoma de México. (2024, abril). Manual de organización de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación. https://www.tic.unam.mx/wp-content/uploads/2024/05/Manual-de-Organizacio%CC%81n-DGTIC-2024.pdf

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 117 - 121

ANEXO A

Para hacer la configuración, primero se elaboraron los *scripts* en un archivo de texto plano (TXT) antes de aplicarlos a los equipos *routers* con los que se reciben los enlaces de red privada virtual empresarial, *LAN-to-LAN* e Internet. Se consideraron las recomendaciones mínimas del fabricante Cisco para el establecimiento de una VPN con túneles GRE más IPSec (Cisco, 2020):

- Cifrado con el algoritmo AES de 128 bits.
- Autenticación con los algoritmos RSA o DSA, ambos de 3072 bits.
- Integridad con el algoritmo SHA de 256 bits.
- Intercambio de llaves con el algoritmo Grupo 15 de 3072 bits de Diffie-Hellman (DH).

Estos parámetros del perfil de IPSec son incluso recomendados por el Centro Nacional de Ciberseguridad del Reino Unido (NCSC por sus siglas en inglés) para proveer seguridad a la transmisión de datos (NCSC, 2022, pp. 7-8), aunque con ciertas reservas que deben ser observadas con detenimiento, dependiendo del contexto de cada implementación.

De acuerdo con las recomendaciones de Hadood (2024), el siguiente procedimiento es una buena práctica para establecer una VPN *Site-to-Site* en equipos Cisco:

1. Definir las credenciales ISAKMP para el intercambio de llaves.
2. Definir las credenciales de IPSec para el intercambio de datos o información.
3. Definir el tráfico de interés para el cifrado a través de una *access-list*.
4. Hacer el *mapping* de todas las credenciales de la VPN en un *crypto map*.
5. Aplicar el *crypto map* a una interfaz (p. 2305).

Para el paso 1, se hace uso del protocolo de asociación de seguridad de Internet y de administración de llaves (ISAKMP por sus siglas en inglés), que sirve para establecer un túnel seguro para la autenticación de dos dispositivos en una primera fase, mientras que, en una fase 2, se encarga de negociar los parámetros de seguridad (llaves y algoritmos, llamados *Security Associations*) para el cifrado de la información. ISAKMP también es llamado IKE y hay dos versiones disponibles (Cisco, 2024). En esta propuesta, se emplea la versión 1 de IKE y, siguiendo las recomendaciones del fabricante ya mencionadas, la configuración sería similar a la que a continuación se muestra:

```
!
crypto isakmp policy 10
 encr aes
 hash sha256
 authentication pre-share
 group 15
!
crypto isakmp key LLAVE_PARA_AUTENTICACIÓN address DIRECCIÓN_IP_ROUTER_REMOTO
!
```

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 118 - 121

Es importante mencionar que, por motivos de confidencialidad y seguridad, no se ejemplifican configuraciones actualmente en operación, sino que son las mínimas recomendadas por Cisco y el gobierno del Reino Unido.

Para el paso 2, como lo recomienda Salman (2017), se determina un *transformation set* que combina la autenticación y el cifrado de los datos (pp. 857-858). En el caso de esta propuesta, se especifica que será en modo túnel, como se muestra en el siguiente ejemplo, de acuerdo con las recomendaciones mínimas del fabricante Cisco:

```
!
crypto ipsec transform-set NOMBRE_DE_TRANSFORMATION_SET esp-aes esp-sha256-hmac
 mode tunnel
!
```

Para el paso 3 es necesario determinar las reglas que permitan la selección del tráfico que se desea hacer pasar por el túnel, que, en esta propuesta, es el tráfico destinado a comunicarse en RedUNAM, mientras que el resto del tráfico es el que debe enrutarse a Internet. Debido a que la idea es conectar el tráfico mediante el protocolo de enrutamiento OSPF con el túnel VPN simulando una conexión directa, se utiliza la tabla de enrutamiento *default* para que el camino hacia RedUNAM se elija por OSPF (hacia el Campus CU) y el camino a Internet se vea por el protocolo BGP (hacia los proveedores de Internet). Ello significa que, para esta propuesta, no es necesario configurar una *access-list* para seleccionar el tráfico que debe pasar por la VPN, ya que de eso se encargará el enrutamiento por sí mismo.

Si bien no es necesaria la lista de acceso para seleccionar el tráfico que transitará por el túnel VPN, sí se emplea una para que las redes locales con máscaras de red mayores a 24 bits utilicen un NAT con las direcciones IP de los ISP, de forma que sí tengan acceso a Internet, sorteando la limitación de la propagación de redes con máscara de hasta 24 bits en Internet. En esta propuesta de VPN, las dos técnicas sencillas son negar el tráfico que sea destinado a RedUNAM y permitir el tráfico de las redes locales con máscaras mayores a 24 bits que vayan a cualquier destino. La configuración ejemplo es la siguiente:

```
!
ip access-list extended LISTA_DE_ACCESO_PARA_EL_NAT_A_INTERNET
 deny   ip any X.X.X.X X.X.X.X
 deny   ip any Y.Y.Y.Y Y.Y.Y.Y
 permit ip L.L.L.L L.L.L.L any
 permit ip M.M.M.M M.M.M.M any
 permit ip N.N.N.N N.N.N.N any
!
```

En donde X.X.X.X y Y.Y.Y.Y son los segmentos de red y su *wildcard* a la que no queremos llegar para salir a Internet, y L.L.L.L, M.M.M.M y N.N.N.N son las redes locales y sus *wildcards* con máscara de red mayor a 24 bits que requieren acceder a Internet mediante el NAT.

Para concluir con la definición de las reglas del NAT, se especifica la interfaz del *router* que conecta el enlace de Internet como salida para el NAT, además de que con un *route-map* se indica que el tráfico, que sea seleccionado por la lista de acceso definida previamente, se dirija por las interfaces de salida del NAT, para que así el tráfico sea enmascarado con la IP del proveedor del enlace:

```
!
interface GigabitEthernet0/1
 ip nat outside
!
```

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 119 - 121

```
route-map NAT_A_INTERNET permit 10
 match ip address LISTA_DE_ACCESO_PARA_EL_NAT_A_INTERNET
 match interface GigabitEthernet0/1
!
ip nat inside source route-map NAT_A_INTERNET interface GigabitEthernet0/1 overload
!
```

Para el paso 4, se debe hacer el *mapping* de las credenciales o parámetros de la VPN en un elemento que se llama *crypto map*, pero, en el caso de esta propuesta de VPN que emplea el modo túnel de IPSec, se usa un perfil con los mismos parámetros del *transform set* previamente definido, para que posteriormente, dicho perfil sea aplicado a las interfaces que se necesiten en el paso siguiente. Las configuraciones básicas recomendadas son las que a continuación se muestran:

```
!
crypto ipsec profile PERFIL_IPSEC_PARA_CIFRADO
 set transform-set NOMBRE_DE_TRANSFORMATION_SET
!
```

Para el último paso 5, se aplica el *crypto map* a las interfaces que sean objeto de la VPN, aunque, en el caso de esta propuesta, se trata del perfil definido previamente. Como se mencionó al principio, la idea es que se emplee un túnel GRE para discernir la comunicación a RedUNAM de la que es dirigida a Internet. Primeramente, se configura una interfaz túnel en cada *router* de los extremos, considerando las direcciones IP de los proveedores de Internet que reciben esos enlaces y que se utilizarán como la red de transporte sobre la que se construye el túnel, además del direccionamiento IP que enumerará ambas puntas para el establecimiento del intercambio de tráfico mediante el protocolo OSPF. Para evitar intermitencia en el establecimiento de la VPN, se debe configurar una ruta estática para alcanzar la IP destino con la que se construye el túnel. Las configuraciones siguientes ejemplifican este paso:

Equipo *router* remoto

```
!
ip route U.U.U.U U.U.U.U GigabitEthernet0/0 I.I.I.1 name IP_TUNNEL_A_SITIO_CENTRAL
!
interface Tunnel1
 description TUNNEL_A_SITIO_CENTRAL
 ip address Z.Z.Z.2 Z.Z.Z.Z
 tunnel source I.I.I.2
 tunnel destination U.U.U.2
!
```

Equipo *router* central

```
!
ip route I.I.I.I I.I.I.I GigabitEthernet0/0 U.U.U.1 name IP_TUNNEL_A_SITIO_REMOTO
!
interface Tunnel1
 description TUNNEL_A_SITIO_REMOTO
 ip address Z.Z.Z.1 Z.Z.Z.Z
 tunnel source U.U.U.2
 tunnel destination I.I.I.2
!
```

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 120 - 121

En donde I.I.I.I y U.U.U.U son las IP y sus máscaras de red del enlace de Internet en cada extremo de la comunicación sobre los cuales se construye el túnel VPN, mientras que Z.Z.Z.Z es el segmento de red de interconexión entre los dos *routers* de cada punta para el intercambio de tráfico a través del protocolo OSPF. La configuración del protocolo OSPF se ejemplifica a continuación:

```
!
router ospf 1
 network Z.Z.Z.Z Z.Z.Z.Z area 0.0.0.0
!
```

Finalmente, se aplica el perfil de IPSec a las interfaces túneles para que se cifre el tráfico que va destinado, en el caso de esta propuesta de VPN, a RedUNAM:

Equipo *router* remoto

```
!
interface Tunnel1
 description TUNNEL_A_SITIO_CENTRAL
 tunnel protection ipsec profile PERFIL_IPSEC_PARA_CIFRADO
!
```

Equipo *router* central

```
!
interface Tunnel1
 description TUNNEL_A_SITIO_REMOTO
 tunnel protection ipsec profile PERFIL_IPSEC_PARA_CIFRADO
!
```

Como paso extra y último de esta propuesta de VPN, se aplica el NAT en las interfaces del *router* de ambos extremos que tengan las redes locales con máscaras mayores a 24 bits para que salgan a Internet con las IP de los proveedores de esos enlaces:

```
!
interface INTERFAZ_LAN_1
 ip tcp adjust-mss 1370
 ip nat inside
!
```

Es importante no olvidar que se debe configurar el ajuste del tamaño del paquete, ya que, conforme se añaden protocolos y sus encabezados, como lo son GRE y el propio IPSec, se incrementa su tamaño, por lo que, para evitar la fragmentación que ocasiona problemas en las aplicaciones, el fabricante Cisco recomienda hacer modificaciones del tamaño de la MTU en la interfaz física, habilitar la negociación del tamaño de MTU automático en los túneles o aplicar directamente el tamaño en las interfaces de los *routers* donde se origine el tráfico que cruzará por la VPN (Cisco, 2023). En el caso de esta propuesta, se determinó que el número de bytes es de 1370, una vez hecho el análisis del tamaño de los encabezados y pruebas con los equipos de cómputo desde las redes locales de algunos sitios para acceder a las aplicaciones de Internet y RedUNAM.

Para finalizar, es recomendable agregar una capa de seguridad al equipo que tenga la VPN configurada, en este caso, un *router*. Obviamos que debe existir un usuario y contraseña exclusivos para acceder

https://doi.org/10.22201/dgtic.30618096e.2025.3.3.125 **Vol. 3, Núm. 3.** julio-septiembre 2025, págs. 121 - 121

al dispositivo, ya sea configurado localmente o mediante un servidor que centralice ese control. La restricción de acceso al equipo se puede implementar de forma sencilla con una lista de control de acceso para permitir sólo a las IP puntuales que deberán tener la autorización para ingresar al equipo:

```
!
username usuario_autorizado secret contrasenia_usuario_autorizado
!
ip access-list standard ACL_ACCESO_REMOTO
 permit X.X.X.X 0.0.0.0
 permit Y.Y.Y.Y 0.0.0.0
 permit Z.Z.Z.Z 0.0.0.0
!
line con 0
 login local
 access-class ACL_ACCESO_REMOTO in
!
line vty 0 4
 login local
 access-class ACL_ACCESO_REMOTO in
!
```

También puede considerarse la implementación de la iniciativa MANRS de la ISOC para tratar de lograr un enrutamiento más seguro en Internet. No se profundiza en esta capa adicional de seguridad, ya que escapa del ámbito principal y de la propuesta de solución de VPN de este reporte técnico.