Estableciendo Conectividad con el AMM para la Entrega de Medición Comercial

Versión 1.5

Última revisión: 5 de mayo 2015

Historial de Revisiones

Versión	Cambios importantes	Fecha
1.0	Primera versión.	14/08/2013
1.1	Se agregó que la VPN se puede establecer hacia un equipo VPN del Participante (router o firewall) que soporte las características necesarias	10/09/2013
1.3	Se agregaron distintas modalidades de enlaces VPN y se ampliaron varios temas.	8/10/2013
1.4	Se agregó otra sección, donde se describe los lineamientos del AMM para cambios a VPNs existentes.	11/04/2014
1.5	En base a la Norma NCO 2.7.1.1 se removió la opción de usar un enlace existente de telemetría. Se actualizaron los hipervínculos hacia la página web del AMM.	05/05/2015

1 Introducción

El Sistema de Medición Comercial (SMEC) es utilizado por el Administrador del Mercado Mayorista (AMM) como base para la liquidación de las transacciones comerciales en el Mercado Mayorista de Electricidad de Guatemala. El SMEC utiliza la información proporcionada por la plataforma *PrimeRead*, que a su vez recolecta datos de los medidores comerciales de los Agentes del Mercado.

Los medidores deben reportar sus datos al PrimeRead vía Internet (IP). Además de la dirección IP, el PrimeRead requiere el DeviceID, No. de Serie, y el número de Puerto TCP de cada medidor, entre otra información.

El presente documento tiene como objetivo ayudar al Participante del Mercado con información sobre las distintas alternativas de conectividad con el AMM para entregar datos de Medición Comercial. Cualquiera de las alternativas que elija el Participante se debe implementar apegado a las políticas de redes del AMM. A continuación se describen con mayor detalle las alternativas de conectividad y las políticas de redes.

NOTAS:

i. *Este documento se provee para la conveniencia de los Participantes del Mercado y es sujeto a cambio sin previo aviso. Es responsabilidad del participante asegurarse que tiene la versión más reciente. Este documento puede contener resúmenes de algunas políticas internas.*

ii. *Se puede encontrar mayor información sobre la Medición Comercial en la página http://www.amm.org.gt/portal/?page_id=142#medicin_comercial y en la norma NCC-14 http://www.amm.org.gt/portal/?wpfb_dl=23ncc-14.pdf .*

2 Alternativas de conectividad para la Medición Comercial

Las alternativas de conectividad con el AMM para la entrega de datos de medición comercial son:

1. IP Pública
2. Enlace VPN
    a. Enlace VPN directo entre el AMM y el Participante
    b. Enlace VPN de acceso al AMM por medio de un proveedor de telecomunicaciones
        i. Usado por 1 solo participante
        ii. Usado por varios participantes (genérico)

2.1 IP Pública

Una dirección de IP Pública se puede acceder directamente desde el Internet y *no* se encuentra en los rangos de direcciones IP privadas (http://supportcenter.verio.com/KB/questions.php?questionid=655). El enrutamiento del tráfico IP se realiza a través de un proveedor de servicios de internet (ISP).

Existe la opción de usar una o varias IPs Publicas para la entrega de medición comercial, siempre y cuando el ancho de banda sea congruente con los flujos de información.

2.1.1 Ejemplo - IP Pública y NAT/PAT

Existen distintas topologías posibles con la opción de IP Pública, el ejemplo de la Figura 1 muestra el caso de un Participante con 3 sitios de medición que está usando una sola IP pública para entregar su medición.

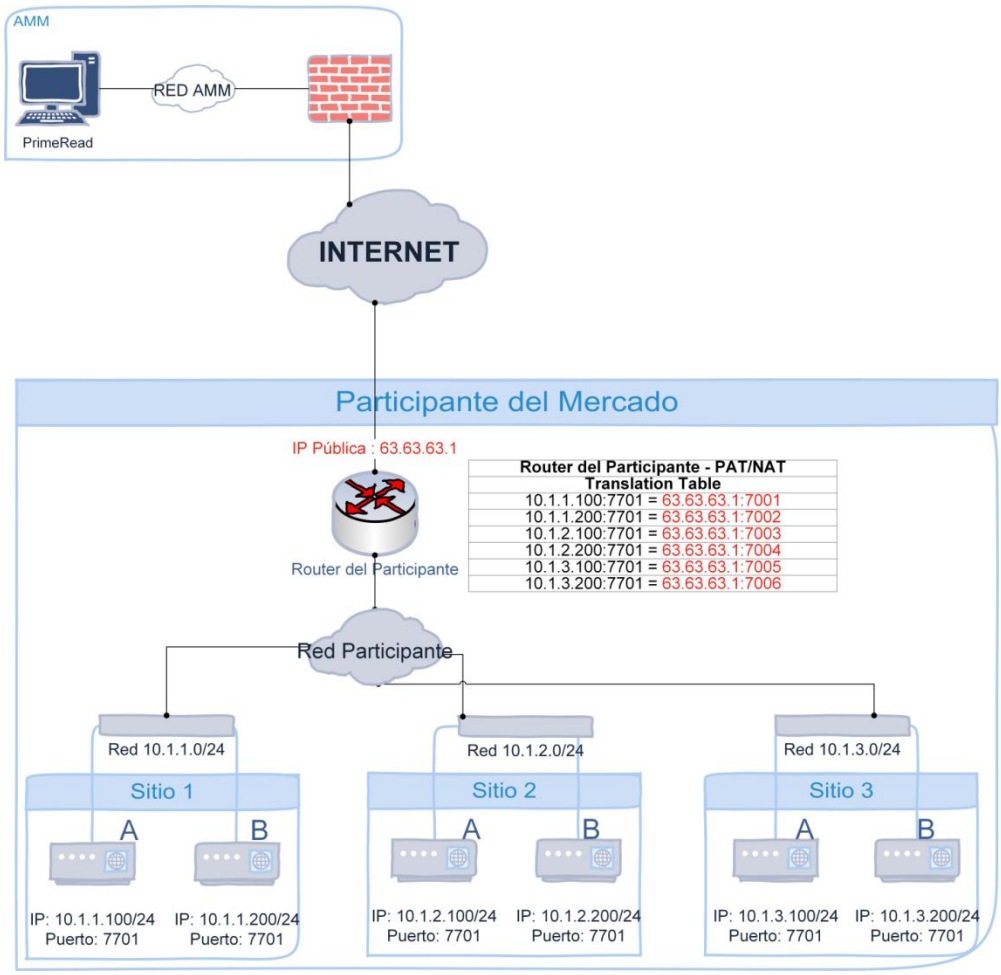
En el ejemplo se usa una configuración de traducción de direcciones de red (NAT) y traducción de direcciones de puerto (PAT) para conectar los medidores de una red privada al Internet usando una sola IP pública.

Las configuraciones de NAT/PAT son soportadas para ciertos modelos de Routers o Firewalls y permitirán que se traduzcan varias direcciones IP privadas de las redes internas del participante hacia una misma IP pública pero con distintos números de puerto.

El participante debe asegurar que su modelo de router o firewall soporta NAT/PAT para esta topología además de cualquier otra especificación necesaria.

El siguiente diagrama muestra una posible topología:

Figura 1



Puramente por razones ilustrativas en el ejemplo se asume que la dirección IP Publica que va a utilizar el Participante para la medición comercial es 63.63.63.1 y que el AMM va a interrogar los medidores usando esta IP pero con diferentes puertos:

Medidor	IP Privada y Puerto del Medidor	IP Publica y Puerto que usaría el AMM para la interrogación
Sitio 1 – Medidor A	**10.1.1.100 : 7701**	**63.63.63.1 : 7001**
Sitio 1 – Medidor B	**10.1.1.200 : 7701**	**63.63.63.1 : 7002**
Sitio 2 – Medidor A	**10.1.2.100 : 7701**	**63.63.63.1 : 7003**
Sitio 2 – Medidor B	**10.1.2.200 : 7701**	**63.63.63.1 : 7004**
Sitio 3 – Medidor A	**10.1.3.100 : 7701**	**63.63.63.1 : 7005**
Sitio 3 – Medidor B	**10.1.3.200 : 7701**	**63.63.63.1 : 7006**

En el ejemplo, cuando el AMM interrogue la dirección IP 63.63.63.1 y puerto 7002 el router del Participante (podría ser también un firewall) traducirá esto en la dirección IP 10.1.1.200 y puerto 7701 que es el medidor B en el sitio 1.

Algunas ventajas de esta configuración son:

- Uso de una sola IP Pública para interrogar varios medidores.
- No hay necesidad de que el AMM tenga conocimiento de las IPs privadas de sus redes internas.
- En su firewall o router podrán agregar seguridad adicional para que solo se acepten interrogaciones de las direcciones IP del AMM.

2.2 Enlace VPN

Un enlace VPN (Virtual Private Network) extiende una red privada a través de una red pública como el Internet. Para establecer un enlace VPN se crea un túnel a través del internet para comunicarse de un extremo a otro de forma segura. Los equipos en los puntos terminales de un enlace VPN generalmente son Firewalls o Routers que soportan distintas configuraciones de VPN y técnicas de seguridad.

El participante puede entregar sus datos de medición comercial por medio de un enlace VPN con el AMM.

Uno de los puntos terminales del enlace VPN será un equipo de Firewall propio del AMM y el otro punto terminal será un equipo VPN (firewalls o routers que soporten VPNs) que puede ser propio del Participante o de su proveedor de servicios de telecomunicaciones. Específicamente, se permiten las siguientes modalidades de enlace VPN:

a. Enlace VPN directo entre el AMM y el Participante
b. Enlace VPN de acceso al AMM por medio de un proveedor de telecomunicaciones
    i. Usado por 1 solo participante
    ii. Usado por varios participantes

A continuación se describen cada una de estas modalidades. Además, en la sección 2.2.3 se describen los requerimientos del AMM para realizar cambios a una VPN existente.

2.2.1 Enlace VPN directo entre el AMM y el Participante

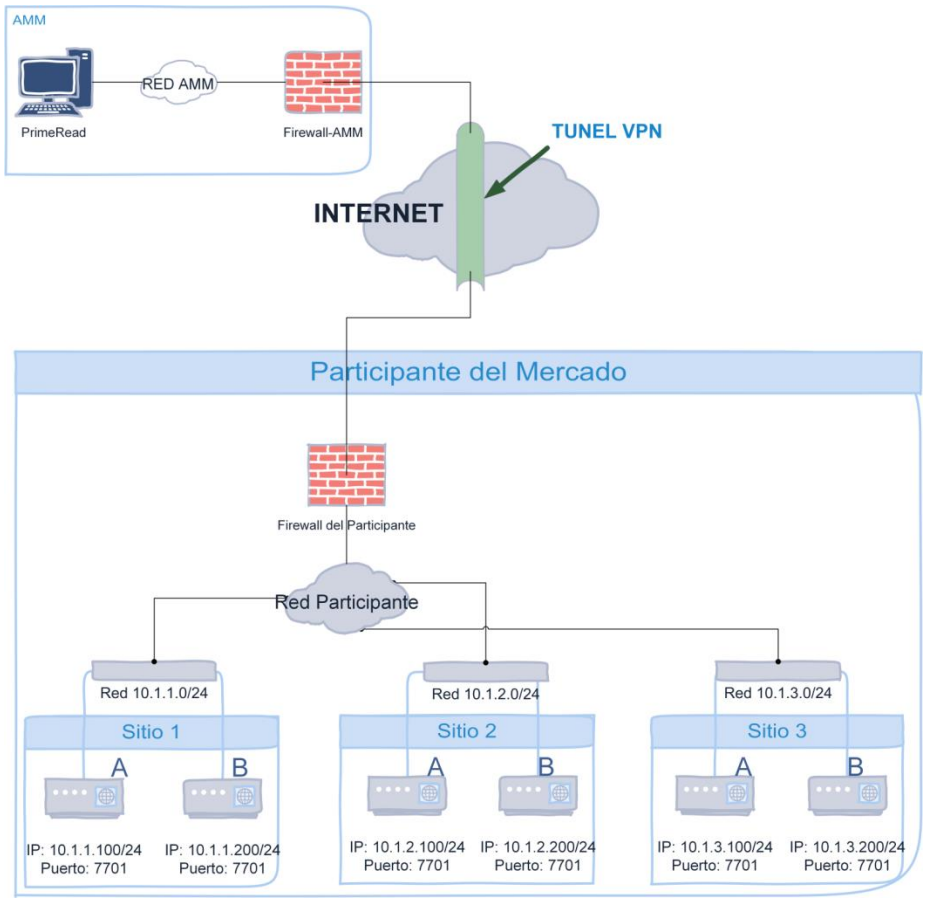
Un enlace VPN directo entre el AMM y el Participante es aquel que se establece directamente entre el equipo de Firewall del AMM y un equipo de Firewall o Router VPN que se encuentra en las instalaciones del Participante y es administrado por él.

El Participante se deberá poner de acuerdo con el AMM para la configuración del enlace VPN y sus pruebas respectivas. Además, el Participante debe asegurar que su modelo de firewall o router soporta la configuración de VPN, NAT, PAT, IKE, e IPSec, además de cualquier otra especificación requerida por el AMM para establecer conectividad.

Esta alternativa es más segura que el de IP Pública, pero el tiempo de implementación puede ser mayor debido a que se deben poner de acuerdo las partes para la configuración y pruebas. Como siempre, existen distintas topologías posibles con esta opción dependiendo de las redes y requerimientos del participante

El ejemplo de la Figura 2 muestra el caso de un Participante con 3 sitios de medición que está usando un enlace VPN directo con el AMM para entregar su medición comercial. El Firewall usado por el participante se encuentra en sus instalaciones y es administrado por él.

Figura 2



2.2.2 Enlace VPN de acceso al AMM por medio de un proveedor de telecomunicaciones

El enlace VPN de acceso al AMM por medio de un proveedor de telecomunicaciones se establece entre el equipo de Firewall del AMM y un equipo de Firewall del proveedor. Luego el proveedor utiliza su red de transmisión para comunicarse con los equipos de medición comercial en distintos puntos. Los enlaces VPN de acceso con el AMM podrán ser de 2 tipos:

i. **Usado por 1 solo participante**: Solo un participante entrega sus datos de medición comercial por el mismo enlace VPN de acceso. La Figura 3 muestra un esquema de este tipo donde el AMM tiene un enlace VPN establecido con el "Proveedor A" de telecomunicaciones. Luego el Proveedor A se conecta por medio de su red únicamente a los medidores del Participante A.

ii. **Usado por varios participantes**: Varios participantes pueden entregar sus datos de medición comercial por medio del mismo enlace VPN de acceso. La Figura 4 muestra un esquema de este tipo donde el AMM tiene un enlace VPN establecido con el "Proveedor A" de telecomunicaciones. Luego, el Proveedor A se conecta por medio de su red a los medidores de los participantes X, Y, y Z.

Figura 3

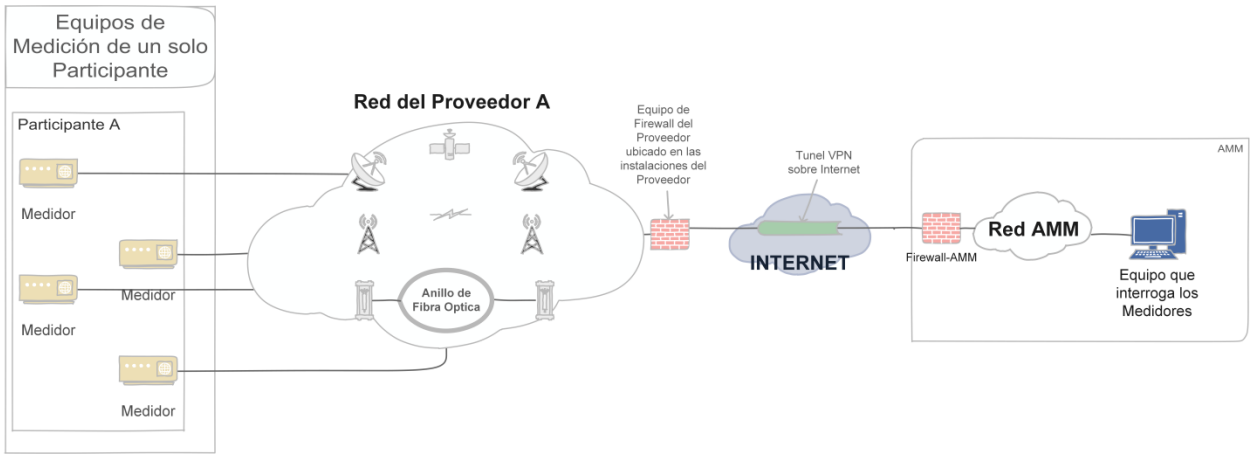
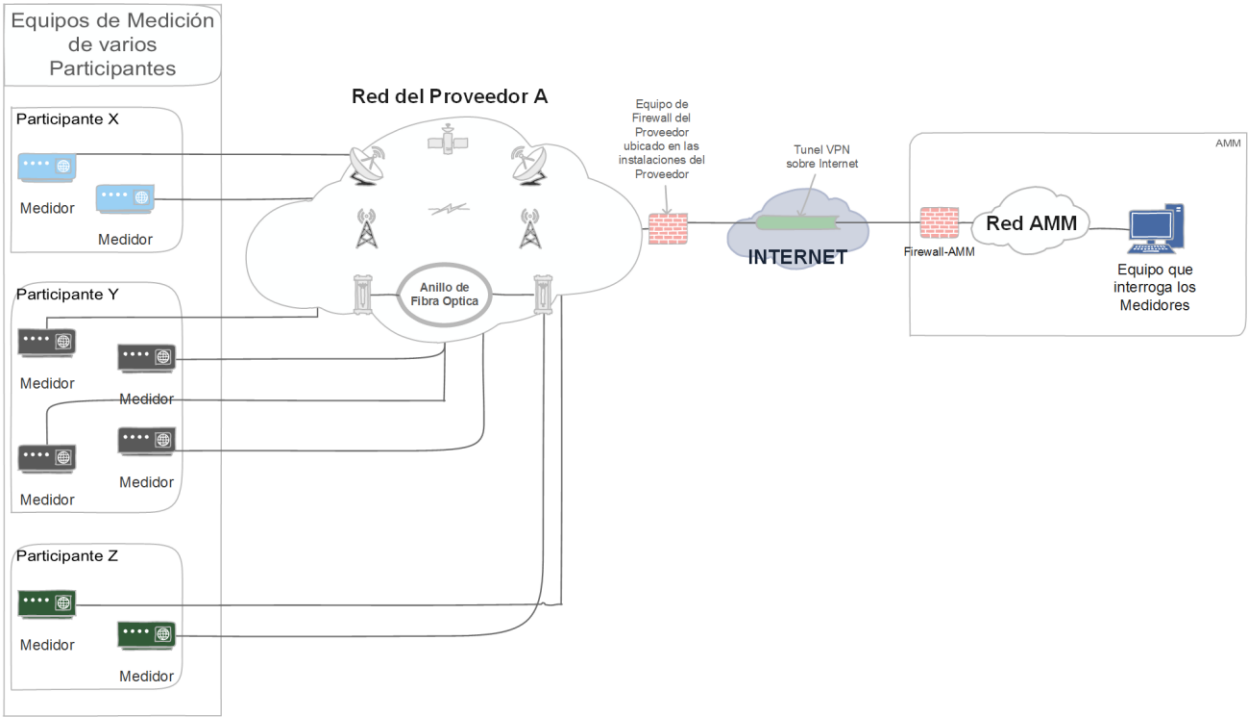


Figura 4



El participante deberá hablar con su proveedor de telecomunicaciones para ver si éste le puede ofrecer estos tipos de soluciones.

Por otra parte, el proveedor de telecomunicaciones se deberá de poner de acuerdo con el AMM para la aprobación de su propuesta. El AMM analizará la factibilidad de la propuesta y quedará en su prerrogativa aprobar o rechazar la misma. De ser aprobada, el AMM y el proveedor realizarán la configuración y pruebas del enlace.

Si el proveedor ya tuviera un enlace VPN de acceso con el AMM del tipo ii que puede ser usado por varios participantes, entonces podría ser más fácil para un participante pegarse a esta solución. Algunos beneficios del segundo esquema son:

- Menor tiempo de implementación
- Uso de infraestructura y configuración existente que se ha probado anteriormente con otros medidores.
- Economía de escala

2.2.3 Requerimientos para cambios a una VPN existente

Si el Participante desea cambiar cualquier parámetro de una VPN existente deberá seguir los siguientes lineamientos del AMM, sin importar la magnitud del cambio.

1. El agente deberá enviar una carta solicitando el cambio a la VPN, y adjuntar a ésta el Formulario de la VPN con los cambios propuestos.

2. Los cambios propuestos a la VPN deben ser previamente aprobados por ambos el Depto. de Medición y el Depto. de Tecnología del AMM.

3. La solicitud de cambio a una VPN debe realizarse con 5 días hábiles de anticipación a la fecha sugerida para el cambio.

4. Los cambios no se pueden realizar en la época de medición, es decir no se podrán programar para los primeros 7 días hábiles del mes.

5. Si los cambios del lado del Agente se programan para un fin de semana o feriado, el Depto. de Medición realizará las pruebas y cambios respectivos hasta el primer día **hábil** de la semana.

6. El Agente se debe comprometer a cumplir con lo siguiente después del cambio:

    a. Realización de la interrogación del 100% de los puntos de medida por parte de la unidad de Aseguramiento de la Medida del Agente para el mes de suministro del cambio de VPN, de acuerdo a los tiempos de cierre de lecturas.

    b. Cumplir con el plazo establecido de 2 días calendario para enviar la información de la totalidad de puntos de medida vía Direct@mm a partir del día que los notifique AMM, de acuerdo al numeral 14.10 de la NCC-14.

    c. Realizar las pruebas necesarias para la sincronización de la VPN una vez realizado el cambio tecnológico a fin de minimizar el impacto del cambio.

3 Políticas de redes

3.1 Generales

1. Las redes propias del AMM no deberán emplearse para subsanar la obligación de un Participante hacia el AMM, ya sea en la entrega de datos de medición comercial, de telemetría en tiempo real u otra. Sin embargo, a criterio del AMM, si podrán emplearse para el transporte de información redundante (de telemetría, de medición comercial, de voz operativa o de otra naturaleza) para asegurar la robustez de sus sistemas, para proporcionar redundancia en donde el Participante no está obligado a proveerla o por criterios técnicos, de seguridad operativa o de importancia estratégica que justifiquen dicho transporte.

2. En ningún caso el transporte de información por parte del AMM eximirá al Participante de sus obligaciones hacia el AMM.

3. El AMM podrá desconectar cualquier equipo de comunicaciones que interfiera (maliciosa o inadvertidamente) con los sistemas del AMM, notificando al Participante para que corrija el elemento. La responsabilidad sobre el cese en los flujos de información recae en el Participante contratante del enlace.

4. En caso de interferencia maliciosa, no se reconectará al Participante hasta que éste documente las causas de la misma, la solución adoptada y subsane los perjuicios que hubiera causado.

5. El AMM podrá adoptar medios de comunicación o esquemas de comunicación no contemplados en este procedimiento siempre que sean analizados y declarados viables, en cuyo caso el respectivo informe será adjuntado al presente procedimiento y los medios analizados pasarán a formar parta de los medios y esquemas aceptados.

6. El AMM podrá desestimar tecnologías, canales de comunicación, o proveedores específicos de comunicaciones si se determina que los mismos no reúnen las condiciones de ancho de bando, confiabilidad, seguridad o robustez necesarias.

3.2 Específicas

1. La telemetría en tiempo real provista por un Agente deberá, de acuerdo a la normativa vigente, entregarse al AMM en canales de comunicación dedicados, ya sea como un flujo individual (DNP3 y protocolos de RTU aprobados en la normativa) o como parte de un flujo colectivo (ICCP). La integración de telemetría se rige por el *Procedimiento de integración de telemetría al SITR* correspondiente.