PBX IP - Seguridad en Publicación de Servicios VoIP

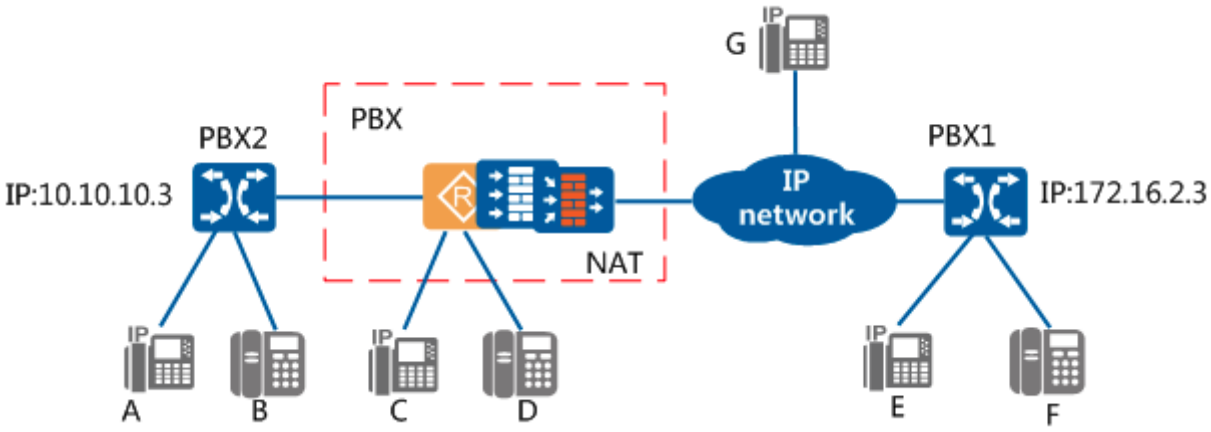
> **Porfavor, LEA DETENIDAMENTE esta guía para no dejar pasar ningún aspecto importante.**

Introducción:

Publicar los servicios SIP (VoIP) de una PBX IP hoy en día suele ser una práctica muy común para brindar mayor flexibilidad a las empresas en cuanto a contectividad con su proveedor de telefonía y sus comunicaciones internas. Sin embargo, hoy en día el "hacking" de plantas PBX IP también es una práctica común por parte de personas desconocidas lo cual genera a fin de mes una sorpresa en la factura del servicio de telefonía. Aquí detallaremos las recomendaciones para la adecuada publicación de servicios VoIP.

Diagrama conceptual de publicación de servicios:

PBX2: Es la sede o ubicación ejemplo donde se publican servicios VoIP mediante un NAT de todos los puertos de una IP pública. Esto con el objetivo que **PBX1** pueda conectarse y exista inter-comunicación entre los teléfonos (A) y (F) sin incurrir en costos de llamadas del proveedor PSTN. También puede haber comunicación entre teléfono (B) y (E) o enlazar una conferencia con (F) también.



Vulnerabilidades:

Si configuramos una IP pública drectamente en la PBX (sin uso de NAT o firewall) estamos exponiendo todos los puertos de la PBX, los cuales pueden tener vulnerabilidades que hasta

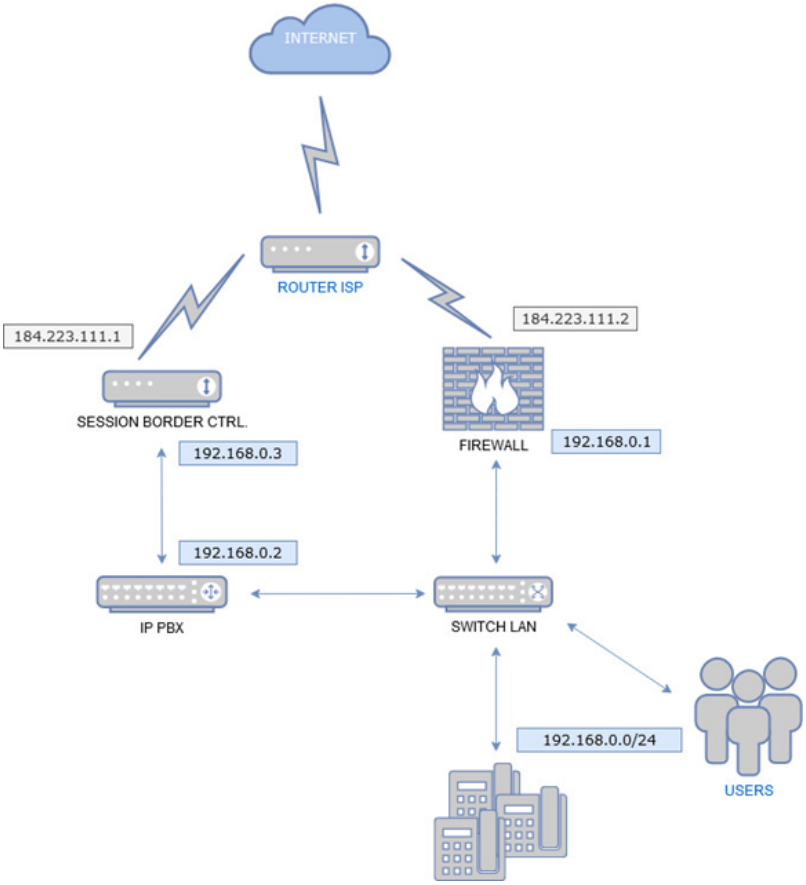
puedan estar documentadas en CVE's oficiales.(https://cve.mitre.org/)

Es por ello que se listan dos soluciones principales:

1. Uso de un Session Border Controller para manejo de sesiones SIP públicas (recomendada)
2. Uso de port forwarding o NAT desde una IP pública hacia la PBX (menos segura)

1) Session Border Controller:

Se han desarrollado equipos destinados a dar la cara por las PBX IP y ser ellos los que reciben ataques y previenen a la PBX de recibirlos directamente. No son firewalls tradicionales, ni routers, son equipos dedicados: Session Border Controllers (SBC) los cuales aparte de contar con características de seguridad y prevención tienen capacidad de manejar codificación del audio para ajustes en el ancho de banda y evitar transcoding dependiendo de la complejidad del entorno VoIP.



Sin embargo, estos equipos por costo suelen ser poco aceptados y los clientes prefieren realizar una publicación de servicios SIP mediante firewalls tradicionales, es por ello que hemos creado una sección en esta guía con las recomendaciones y advertencias de un escenario sin SBC.

2) NAT de puertos VoIP como solución:

Existen alternativas si no se puede adquirir un SBC para la publicación de servicios, una de ellas es realizar un NAT de los servicios VoIP utilizando un firewall que pueda tener cierto control y monitoreo de ataques básicos (no VoIP). Realizar un redireccionamiento de puertos SIP únicamente para la IP interna de la PBX y de ser posible habilitar bloqueo por geolocalización.

Recomendaciones Importantes: Recomendamos realizar los siguientes cumplimientos de manera estricta:

- **Cambiar contraseñas SIP de las extensiones** y que contengan una longitud de 12 dígitos mínimo (de preferencia 16 dígitos), incluyendo al menos cuatro mayúsculas intercaladas entre cinco números y varias minúsculas. **NO utilizar:** palabras diccionario o relacionadas al país o negocio, tampoco relacionadas a la extensión o que lleven correlativos alfanuméricos.
- **NO publicar servicios administrativos HTTP** para la PBX, de preferencia **solo servicio VoIP.** Si fuese requerido el servicio HTTP (por WebRTC u otros) se recomienda habilitarlo en HTTPS para un tráfico cifrado y habilitar además en el firewall políticas de detección de intrusos e inspección de tráfico SSL para mitigar vulnerabilidades.
- Mantener activas las políticas de **Fail2Ban** para que los intentos fallidos sean bloqueados y rechazados. Configurar el bloqueo al menos por 1 hora para intentos fallidos, si es factible aumentar el tiempo a un día mucho que mejor.
- Mantener las **claves administrativas** de los teléfonos IP (equipos) de manera robusta (admin) pues es otra puerta para indagar contraseñas SIP.
- SI es viable, implementar llamadas mediante el uso de TLS para tráfico RTP.
- Habilitar la administración de la PBX (Web, ssh, etc) sólo para un rango de IP's de la red interna, para evitar vulnerabilidades mediante el uso de robots anidados en la red interna de la PBX (PC's, teléfonos, etc).
- Para equipos físicos (appliances) Grandstream, Zycoo y otros se recomienda efectual actualizaciones de firmware periódicamente para mitigar vulnerabilidades en servicios internos (CVE's).

> Pueden configurarse contraseñas con símbolos, esto es muy recomendado, pero ciertos equipos de telefonía no lo soportan, por lo que se deja como una opción deseada y la que se recomienda probar.

En Firewalls y Routers: Deshabilitar el servicio de **SIP ALG,** consulte con el fabricante o su Ingeniero de Soporte sobre como deshabilitar dicho servicio.

Seguridad avanzada en Firewalls: En algunos firewalls como Watchguard o Fortinet, se permite el uso de funcionalidades de bloqueos mediante funciones pagadas o incluídas en la suscripción de los servicios estándar. Se recomienda implementar las funcionalidades siguientes:

- Programar las políticas de Firewall donde se hace el NAT o Port Forwarding con horarios específicos de operación. Un ejemplo puede ser: Deshabilitar tráfico SIP a partir de las 20:00 horas de Lunes a Viernes y en ningún horario para fines de semana.
- Bloquear tráfico de las políticas de Firewall donde se hace NAT o Port Forwarding para las IP's origen de otros territorios, paises o continentes. En Watchguard se denomina "Geolocation Block" y permite seleccionar los países de donde se puede recibir tráfico para dicha política. En Fortinet se denomina "Geo IP Black list" y permite seleccionar los países también. Más información con el fabricante o su Ingeniero de Soporte.

NOTA: NO publicar servicios web u otros puertos hacia la PBX IP, únicamente los servicios antes descritos. Si se publican más servicios o se hace un redireccionamiento completo se pueden vulnerar: Servicios Web, Servicios de Base de Datos, Servicios de Asterisk AMI, Servicios SSH y otros, dependiendo la plataforma de la PBX IP.

Advertencias:

- Los servicios PBX IP publicados mediante IP pública son los destinos más buscados por los hackers, pues estos representan una “mina de oro” para ellos poder negociar con tráfico de llamadas internacional sin costo alguno.
- Existen robots que operan 24x7 los cuales escanean IP’s constantemente para indagar que IPs atienden servicios SIP/VoIP y luego de detectar generan listas para que otros robots lancen ataques SIP para vulnerar cuentas y así poder aterrizar llamadas internacionales en una IP hackeada.
- Es responsabilidad del cliente propietario de la PBX el cumplir con los lineamientos mínimos recomendados en seguridad de la IP PBX.
- Es responsabilidad del cliente cualquier vulnerabilidad que haya sido explotada mediante hackings a su plataforma IP PBX, ya que la publicación de servicios es una práctica que debe ser protegida por Session Border Controllers (Firewalls SIP) y no por firewalls tradicionales, sin embargo se proveen aquí las alternativas para publicar los servicios y proveer la seguridad de la mejor manera posible mediante “mejores prácticas”.

Vox Datacomm, S.A.: NO se hace responsable por servicios vulnerados por terceras personas, tampoco se hace responsable del pago de facturas o servicios de telefonía del cliente final que ha tenido vulnerabilidades en su PBX a causa de no seguir las prácticas recomendadas. La información aquí expuesta y compartida NO supone un compromiso o garantía de que la PBX IP será segura. El cliente o el lector de este documento es el único responsable por la gestión y administración de la PBX y de garantizar su seguridad mediante la revisión periódica y monitoreo constante. Buenas prácticas en el link: AQUÍ.

Revision #25
Created 20 December 2019 16:07:08 by Eduardo Mejia
Updated 30 January 2023 18:05:48 by Eduardo Mejia