Elaborado por:	Revisado por:	Aprobado por:
Vicepresidencia Infraestructura – Gerencia Ingeniería de Red y Servicios – Laboratorio de Ingenieria, Investigación y Desarrollo - William Orlando Girón Mora	Vicepresidencia Infraestructura – Gerencia Ingeniería de Red y Servicios – Cesar Augusto Mendoza Noy	Vicepresidencia Infraestructura – Gerencia Ingeniería de Red y Servicios – Cesar Augusto Mendoza Noy

Tabla de contenido

Introducción

ETB requiere con este documento presentar la base de la elaboración del documento de las Pruebas de Aceptación ATP del Servicio de Ingeniería para la realización de las pruebas técnicas de los equipos objetos del contrato. El 100% de las pruebas técnicas deberán obtener resultados exitosos y de cumplimiento o en acuerdo con personal especializado designado por ETB resultados aceptables o no verificables. Las pruebas que se van a ejecutar reflejan las funcionalidades técnicas requeridas en los términos técnicos del proceso y aceptadas en cumplimiento por el CONTRATISTA.

Objetivos

- Servir como base para la elaboración del documento de pruebas de aceptación ATP, entregable del servicio de ingeniería.
- Realizar pruebas técnicas de aceptación a los equipos objetos del proceso firewall backend dentro de un ambiente controlado ubicado en ETB.
- Determinar si los equipos ofertados cumplen con las funcionalidades requeridas en los términos técnicos del proceso, las cuales fueron aceptadas por el CONTRATISTA, convirtiéndolos aptos para el servicio de firewall backend de ETB.
- Soportar el documento de pruebas de aceptación ATP, hito de pago en el proceso de firewall backend.

Alcance

Este documento se convierte como base de las pruebas de aceptación ATP que se realizarán a los equipos firewalls backend tanto para los equipos firewalls suministrados como para la actual arquitectura Fortinet de ETB objeto del contrato y al sistema de gestión remota centralizada y generación de reportes, si es que aplican por separado. Estos deben ser suministrados, instalados y configurados por el CONTRATISTA para las pruebas.

Definiciones

N/A

Advertencia

Condiciones para la ejecución de las pruebas de aceptación

- Las pruebas se realizarán en días laborales de lunes a viernes en el horario comprendido entre las 7 AM a 5 PM con un receso de una hora para almorzar. Este horario podrá ser extendido por decisión unilateral por parte de ETB.
- Máximo se aceptará la presencia de dos (2) personas en representación del CONTRATISTA.
- El CONTRATISTA garantizará que los equipos en el momento de las pruebas de aceptación posean el software, firmware actualizado, el cual será el empleado en el momento de la migración de la configuración para la puesta en producción.
- El CONTRATISTA pondrá a disposición todo el recurso hardware y software necesarios para la realización de las pruebas, entre otros como generadores de tráfico, equipos tester de las pruebas, máquinas virtuales, software para la virtualización, equipos de cómputo y servidores, entre otros.

- El CONTRATISTA será el responsable de la manipulación del hardware, software y equipos que hace parte de las pruebas de aceptación, tanto como los pertenecientes al objeto del contrato, como los puestos a disposición para las pruebas de aceptación.
- El lugar de realización de las pruebas de aceptación, podrán ser el Datacenter Cuni y Nodo Chico. Por consiguiente, el CONTRATISTA deberá ser responsable del transporte, traslado e ingreso y salida del hardware y software puestos a disposición para la realización de las pruebas de aceptación.
- El CONTRATISTA deberá garantizar la experticia en la configuración y troubleshooting de los equipos de la solución firewall backend en el momento de las pruebas de aceptación.
- En caso de cambios de software, firmware durante la ejecución de las pruebas, será obligatorio volver a empezar el protocolo de pruebas. El CONTRATISTA deberá tener en cuenta que estos reinicios podrán afectar su cumplimiento del cronograma establecido.
- El orden de ejecución de las pruebas son decisión de ETB.
- ETB podrá hacer cambios de forma y de fondo a las pruebas descritas en este protocolo y podrá adicionar, modificar o eliminar pruebas unilateralmente.
- Para las pruebas se determinará los datos específicos de cada equipo como modelo, referencia, serial de todo el hardware y sus componentes modulares y las versiones de software, firmware, parches, actualizaciones o builds, que tenga el equipo. Estos datos deberán ser diligenciados en el siguiente formato.

FABRICANTE	MODELO	REFERENCIA	SERIAL	VERSION DE FIRMWARE	CANTIDAD

1. Pruebas funcionales

1.1. Equipos firewalls nuevos

1.1.1. Pruebas de estrés

Ítem	Pruebas de estrés en los equipos
Propósito	Identificar el rendimiento del equipo en condiciones de tráfico, configuraciones de protección y funciones adicionales de la red interna.
Ambiente de prueba:	
Procedimiento: 1. Conectar el equipo firewall a la red de datos de ETB. 2. Configurar y conectar a la red de pruebas de ETB un generador de tráfico que simule la navegación de un usuario a internet. Ver resultado 1. 3. Simular una implementación del equipo firewall en línea de manera intrusiva en la red. Ver resultado 1. 4. Configurar el equipo firewall con política de firewall default (any-any) aplicando un perfil de antivirus/antispyware con acción de bloqueo al tráfico simulado que fluye por esa regla de firewall. Ver resultado 1. 5. Configurar el equipo FIREWALL con política de firewall default (any-any) aplicando un perfil de IPS con acción de bloqueo al tráfico simulado que fluye por esa regla de firewall. Ver resultado 1.	
Resultados esperados: 1. El equipo firewall no debe presentar decrementos de throughput, perdida de paquetes o tramas.	

Resultados prueba de validación	**Cumple** ☐	**No Cumple** ☐	**No verificado** ☐

Comentarios	• (Se debe escribir los comentarios relevantes a la prueba específica, si se presentaron inconvenientes, si faltaron recursos, problemas en las configuraciones, demoras y sus causas etc.….)	
Responsables:	**Proveedor:** **Firma** _____	**ETB:** **Firma** _____

1.1.2. Pruebas acceso vía CLI

Ítem	Acceso via Command Line Interface (CLI)
Propósito	Acceso a los equipos para gestión por la Interfaz de Línea de Comandos (CLI), a través de puerto Consola y protocolo SSH.

Ambiente de prueba:

(Diagrama del Escenario de Prueba)

Procedimiento:

1. Configurar los equipos firewalls con una dirección IPv4 para gestión vía consola.
2. Conectar cable de consola al puerto Console del equipo firewall usando la aplicación Putty ó aplicaciones similares. Ver resultado 1.
3. Conectar el equipo firewall a la red de pruebas de ETB por medio de cable UTP. Ver resultado 2.

Resultados esperados:

1. Se debe acceder a los equipos firewalls por el puerto Console y en la aplicación observar la solicitud de credenciales. Al ingresar las credenciales debe observarse la configuración del sistema.
2. Se debe acceder a los equipos firewalls a través de la dirección IP de gestión por el protocolo SSH y en la aplicación observar la solicitud de credenciales. Al ingresar las credenciales debe observarse la configuración del sistema.
3. Observar la versión del software, fimware, parche o build, el cual debe coincidir con el informado al inicio de las pruebas.

Resultados prueba de validación	**Cumple** ☐	**No Cumple** ☐	**No verificado** ☐
Comentarios	• (Se debe escribir los comentarios relevantes a la prueba específica, si se presentaron inconvenientes, si faltaron recursos, problemas en las configuraciones, demoras y sus causas etc.….)		
Responsables:	**Proveedor:** **Firma** _____	**ETB:** **Firma** _____	

1.1.3. Control de conexiones

Ítem	Control de conexiones
Propósito	Comprobar el control de conexiones a través de reglas de firewall.
Ambiente de prueba:	

Procedimiento:

1. Configurar el ambiente de prueba con el equipo firewall en línea, de tal manera el tráfico internet del computador cruce a través de el.
2. Configurar una regla de firewall que permita la salida del computador hacia internet, pero que bloquee el puerto TCP 80.
3. Realizar las configuraciones necesarias en el equipo firewall.
4. Conectar el equipo firewall a la red de pruebas.
5. Desde el computador conectado en la Red LAN navegar hacia internet.

Resultados esperados:

1. El computador podrá navegar hacia internet a través de cualquier protocolo como HTTPS o FTP, y no podrá navegar a través del protocolo TCP 80 HTTP.
2. Visualizar estadísticas de navegación por:
   a. Consumo por puertos (TCP/UDP)
   b. Conexiones establecidas.
   c. Throughput.
   d. Bloqueo del tráfico por el puerto TCP 80.

Resultados prueba de validación	**Cumple** ☐	**No Cumple** ☐	**No verificado** ☐
Comentarios	• (Se debe escribir los comentarios relevantes a la prueba específica, si se presentaron inconvenientes, si faltaron recursos, problemas en las configuraciones, demoras y sus causas etc.….)		
Responsables:	**Proveedor:** **Firma** _____	**ETB:** **Firma** _____	

1.1.4. Pruebas IPS

Ítem	Sistema de prevención de intrusos (IPS)		
Propósito	Comprobar la protección perimetral a través de un perfil de IPS aplicado al tráfico internet.		
Ambiente de prueba:			
Procedimiento: 1. Configurar el ambiente de prueba con el equipo firewall en línea, de tal manera el tráfico internet del computador cruce a través de el. 2. Configurar una regla de firewall que permita la salida del computador hacia internet. A esta regla de firewall o tráfico que fluye a través de esta regla se le debe aplicar un perfil de IPS default, entendiéndose default como firmas IPS y acciones de estas firmas de IPS default del sistema operativo sin afinamiento manual. 3. Realizar las configuraciones necesarias en el equipo firewall. 4. Conectar el equipo firewall a la red de pruebas. 5. Desde el computador conectado en la Red LAN navegar hacia internet de manera maliciosa hacia un destino externo de la red LAN, o en su defecto generar trafico malicioso desde el computador conectado en la Red LAN hacia un destino conectado directamente en L1 o L2 antes del router.			
Resultados esperados: 1. El tráfico que hace coincidencia con firmas de IPS es bloqueado o detectado por el FIREWALL. 2. Visualizar estadísticas o logs de: a. Tráfico bloqueado o detectado. b. Firmas que bloquearon o detectaron el tráfico.			
Resultados prueba de validación	**Cumple** ☐	**No Cumple** ☐	**No verificado** ☐
Comentarios	• (Se debe escribir los comentarios relevantes a la prueba específica, si se presentaron inconvenientes, si faltaron recursos, problemas en las configuraciones, demoras y sus causas etc.….)		

Responsables:	Proveedor:	ETB:
	Firma _____	Firma _____

1.1.5. Prueba de Antivirus

Ítem	Antivirus/Antispyware perimetral		
Propósito	Comprobar la protección perimetral a través de un perfil de Antivirus/Antispyware aplicado al tráfico internet.		
Ambiente de prueba:			
Procedimiento: 1. Configurar el ambiente de prueba con el equipo FIREWALL en línea, de tal manera el tráfico internet del computador cruce a través de el. 2. Configurar una regla de firewall que permita la salida del computador hacia internet. A esta regla de firewall o tráfico que fluye a través de esta regla de firewall se le debe aplicar un perfil de Antivirus perimetral con acción de bloqueo. 3. Conectar el equipo FIREWALL a la red de pruebas. 4. Desde el computador conectado en la Red LAN navegar hacia internet. 5. Enviar o recibir en el computador conectado a la red LAN, el archivo con contenido malware a través de HTTP o FTP. Ver resultado esperado 1 y 2.			
Resultados esperados: 1. El tráfico que contenga malware es bloqueado por el FIREWALL. 2. Visualizar estadísticas o logs de: a. Tráfico bloqueado.			
Resultados prueba de validación	**Cumple** ☐	**No Cumple** ☐	**No verificado** ☐
Comentarios	• (Se debe escribir los comentarios relevantes a la prueba específica, si se presentaron inconvenientes, si faltaron recursos, problemas en las configuraciones, demoras y sus causas etc.….)		

Responsables:	Proveedor:	ETB:
	Firma _____	Firma _____

1.1.6. VPN SSL Client to Site

Ítem	VPN SSL Client to Site
Propósito	Comprobar la funcionalidad de VPN SSL Client to Site, a través de portal WEB y con agente instalado en el computador.

Ambiente de prueba:

Procedimiento:

1. Configurar el ambiente de prueba con el equipo FIREWALL conectado a la red de pruebas de tal manera el computador se vea lógicamente con el equipo FIREWALL a través de un router garantizando que se ubiquen en diferentes segmentos de red.
2. Configurar una interfaz loopback con una dirección IP no enrutada a través del router.
3. Realizar las configuraciones necesarias en el equipo FIREWALL para lograr los resultados esperados.
4. Validar el resultado esperado 1.
5. Instalar y configurar el agente VPN SSL en el computador el cual debe ser propietario de la marca del FIREWALL.

Resultados esperados: 1. Sin establecer la VPN SSL con el equipo FIREWALL, el computador no alcanza lógicamente la dirección IP de la interfaz loopback. 2. El computador deberá establecer a través del agente VPN SSL activo, una VPN SSL con el FIREWALL y alcanzar la dirección IP de la interfaz loopback 3. Sin establecer la VPN SSL con el equipo FIREWALL, el computador no alcanza lógicamente la dirección IP de la interfaz loopback. 4. Con el agente inactivo o desinstalado, el computador podrá acceder a una página web publicada por el FIREWALL a través del protocolo HTTPS con protocolo de cifrado TLS 1.2 o 1.3 y establecer una VPN SSL a través de ese portal WEB. Una vez establecida la VPN SSL podrá alcanzarla dirección IP de la interfaz loopback.			
Resultados prueba de validación	**Cumple** ☐	**No Cumple** ☐	**No verificado** ☐
Comentarios	• (Se debe escribir los comentarios relevantes a la prueba específica, si se presentaron inconvenientes, si faltaron recursos, problemas en las configuraciones, demoras y sus causas etc.….)		
Responsables:	**Proveedor:** **Firma** _____	**ETB:** **Firma** _____	

1.2. Equipos Firewalls Fortinet

1.2.1. Pruebas acceso vía CLI

Ítem	Acceso via Command Line Interface (CLI)
Propósito	Acceso a los equipos para gestión por la Interfaz de Línea de Comandos (CLI), a través de puerto Consola y protocolo SSH.
Ambiente de prueba: (Diagrama del Escenario de Prueba)	

Procedimiento:

4. Configurar los equipos firewalls con una dirección IPv4 para gestión vía consola.
5. Conectar cable de consola al puerto Console del equipo firewall usando la aplicación Putty ó aplicaciones similares. Ver resultado 1.
6. Conectar el equipo firewall a la red de pruebas de ETB por medio de cable UTP. Ver resultado 2.

Resultados esperados:

4. Se debe acceder a los equipos firewalls por el puerto Console y en la aplicación observar la solicitud de credenciales. Al ingresar las credenciales debe observarse la configuración del sistema.
5. Se debe acceder a los equipos firewalls a través de la dirección IP de gestión por el protocolo SSH y en la aplicación observar la solicitud de credenciales. Al ingresar las credenciales debe observarse la configuración del sistema.
6. Observar la versión del software, fimware, parche o build, el cual debe coincidir con el informado al inicio de las pruebas.

Resultados prueba de validación	**Cumple** ☐	**No Cumple** ☐	**No verificado** ☐
Comentarios	• (Se debe escribir los comentarios relevantes a la prueba específica, si se presentaron inconvenientes, si faltaron recursos, problemas en las configuraciones, demoras y sus causas etc.….)		
Responsables:	**Proveedor:** **Firma** _____	**ETB:** **Firma** _____	

1.2.2. Control de conexiones

Ítem	Control de conexiones		
Propósito	Comprobar el control de conexiones a través de reglas de firewall.		
Ambiente de prueba:			
Procedimiento: 6. Configurar el ambiente de prueba con el equipo firewall en línea, de tal manera el tráfico internet del computador cruce a través de el. 7. Configurar una regla de firewall que permita la salida del computador hacia internet, pero que bloquee el puerto TCP 80. 8. Realizar las configuraciones necesarias en el equipo firewall. 9. Conectar el equipo firewall a la red de pruebas. 10. Desde el computador conectado en la Red LAN navegar hacia internet.			
Resultados esperados: 3. El computador podrá navegar hacia internet a través de cualquier protocolo como HTTPS o FTP, y no podrá navegar a través del protocolo TCP 80 HTTP. 4. Visualizar estadísticas de navegación por: a. Consumo por puertos (TCP/UDP) b. Conexiones establecidas. c. Throughput. d. Bloqueo del tráfico por el puerto TCP 80.			
Resultados prueba de validación	**Cumple** ☐	**No Cumple** ☐	**No verificado** ☐
Comentarios	• (Se debe escribir los comentarios relevantes a la prueba específica, si se presentaron inconvenientes, si faltaron recursos, problemas en las configuraciones, demoras y sus causas etc.….)		

Responsables:	Proveedor:	ETB:
	Firma _____	Firma _____

1.2.3. Pruebas IPS

Ítem	Sistema de prevención de intrusos (IPS)
Propósito	Comprobar la protección perimetral a través de un perfil de IPS aplicado al tráfico internet.

Ambiente de prueba:

Procedimiento:

6. Configurar el ambiente de prueba con el equipo firewall en línea, de tal manera el tráfico internet del computador cruce a través de el.
7. Configurar una regla de firewall que permita la salida del computador hacia internet. A esta regla de firewall o tráfico que fluye a través de esta regla se le debe aplicar un perfil de IPS default, entendiéndose default como firmas IPS y acciones de estas firmas de IPS default del sistema operativo sin afinamiento manual.
8. Realizar las configuraciones necesarias en el equipo firewall.
9. Conectar el equipo firewall a la red de pruebas.
10. Desde el computador conectado en la Red LAN navegar hacia internet de manera maliciosa hacia un destino externo de la red LAN, o en su defecto generar trafico malicioso desde el computador conectado en la Red LAN hacia un destino conectado directamente en L1 o L2 antes del router.

Resultados esperados: 3. El tráfico que hace coincidencia con firmas de IPS es bloqueado o detectado por el FIREWALL. 4. Visualizar estadísticas o logs de: a. Tráfico bloqueado o detectado. b. Firmas que bloquearon o detectaron el tráfico.			
Resultados prueba de validación	**Cumple** ☐	**No Cumple** ☐	**No verificado** ☐
Comentarios	• (Se debe escribir los comentarios relevantes a la prueba específica, si se presentaron inconvenientes, si faltaron recursos, problemas en las configuraciones, demoras y sus causas etc.….)		
Responsables:	**Proveedor:** **Firma** _____	**ETB:** **Firma** _____	

1.2.4. Prueba de Antivirus

Ítem	Antivirus/Antispyware perimetral
Propósito	Comprobar la protección perimetral a través de un perfil de Antivirus/Antispyware aplicado al tráfico internet.
Ambiente de prueba:	

Procedimiento:

6. Configurar el ambiente de prueba con el equipo FIREWALL en línea, de tal manera el tráfico internet del computador cruce a través de el.
7. Configurar una regla de firewall que permita la salida del computador hacia internet. A esta regla de firewall o tráfico que fluye a través de esta regla de firewall se le debe aplicar un perfil de Antivirus perimetral con acción de bloqueo.
8. Conectar el equipo FIREWALL a la red de pruebas.
9. Desde el computador conectado en la Red LAN navegar hacia internet.
10. Enviar o recibir en el computador conectado a la red LAN, el archivo con contenido malware a través de HTTP o FTP. Ver resultado esperado 1 y 2.

Resultados esperados:

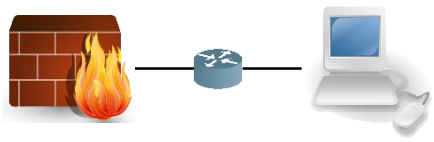
3. El tráfico que contenga malware es bloqueado por el FIREWALL.
4. Visualizar estadísticas o logs de:
   a. Tráfico bloqueado.

Resultados prueba de validación	**Cumple** ☐	**No Cumple** ☐	**No verificado** ☐
Comentarios	• (Se debe escribir los comentarios relevantes a la prueba específica, si se presentaron inconvenientes, si faltaron recursos, problemas en las configuraciones, demoras y sus causas etc.….)		
Responsables:	**Proveedor:** **Firma** _____	**ETB:** **Firma** _____	

1.2.5. VPN SSL Client to Site

Ítem	VPN SSL Client to Site
Propósito	Comprobar la funcionalidad de VPN SSL Client to Site, a través de portal WEB y con agente instalado en el computador.

Ambiente de prueba:



Procedimiento: 6. Configurar el ambiente de prueba con el equipo FIREWALL conectado a la red de pruebas de tal manera el computador se vea lógicamente con el equipo FIREWALL a través de un router garantizando que se ubiquen en diferentes segmentos de red. 7. Configurar una interfaz loopback con una dirección IP no enrutada a través del router. 8. Realizar las configuraciones necesarias en el equipo FIREWALL para lograr los resultados esperados. 9. Validar el resultado esperado 1. 10. Instalar y configurar el agente VPN SSL en el computador el cual debe ser propietario de la marca del FIREWALL.			
Resultados esperados: 5. Sin establecer la VPN SSL con el equipo FIREWALL, el computador no alcanza lógicamente la dirección IP de la interfaz loopback. 6. El computador deberá establecer a través del agente VPN SSL activo, una VPN SSL con el FIREWALL y alcanzar la dirección IP de la interfaz loopback 7. Sin establecer la VPN SSL con el equipo FIREWALL, el computador no alcanza lógicamente la dirección IP de la interfaz loopback. 8. Con el agente inactivo o desinstalado, el computador podrá acceder a una página web publicada por el FIREWALL a través del protocolo HTTPS con protocolo de cifrado TLS 1.2 o 1.3 y establecer una VPN SSL a través de ese portal WEB. Una vez establecida la VPN SSL podrá alcanzarla dirección IP de la interfaz loopback.			
Resultados prueba de validación	**Cumple** ☐	**No Cumple** ☐	**No verificado** ☐
Comentarios	• (Se debe escribir los comentarios relevantes a la prueba específica, si se presentaron inconvenientes, si faltaron recursos, problemas en las configuraciones, demoras y sus causas etc.….)		
Responsables:	**Proveedor:** **Firma** _____	**ETB:** **Firma** _____	

1.3. Sistema de gestión centralizada y reportes

1.3.1. Actualizaciones

Ítem	Actualización de firmware		
Propósito	Ejecutar el proceso de actualización del sistema operativo y firmware del firewall desde el sistema de gestión centralizada y reportes		
Ambiente de prueba:			
Procedimiento: 1. Realizar las configuraciones necesarias en el equipo FIREWALL. 2. Conectar el equipo FIREWALL a la red de pruebas e integrarlo con el sistema de gestión centralizada y reportes. 3. Generar actualización de Firmware desde el sistema de gestión centralizada y reportes al equipo firewall.			
Resultados esperados: 1. Validar el funcionamiento de la administración desde el sistema de gestión centralizada y reportes.			
Resultados prueba de validación	**Cumple** ☐	**No Cumple** ☐	**No verificado** ☐
Comentarios	• (Se debe escribir los comentarios relevantes a la prueba específica, si se presentaron inconvenientes, si faltaron recursos, problemas en las configuraciones, demoras y sus causas etc.….)		
Responsables:	**Proveedor:** **Firma** _____	**ETB:** **Firma** _____	

1.3.2. Privilegios de niveles de usuarios

Ítem	Acceso a reportes y privilegios de niveles de usuario.
Propósito	Verificar la forma de acceso segura a la solución de gestión y reportes

Ambiente de prueba:

Procedimiento:

1. Configurar el ambiente de prueba con el equipo FIREWALL en línea, de tal manera el tráfico hacia internet del computador cruce a través de el.
2. Conectar el equipo FIREWALL a la red de pruebas.
3. Conectar la plataforma de gestión y de reportes al escenario de pruebas.
4. Configurar la red de pruebas para lograr los resultados esperados.
   a. Switching
   b. Routing
   c. SNMP Server
   d. NTP Server
5. Realizar las configuraciones necesarias en el equipo FIREWALL y en la plataforma de gestión y reportes.

Resultados esperados:

1. Tener acceso a la solución de la plataforma de gestión y reportes a través de HTTPS desde el computador o desde el cliente/servidor. Ingresar a la plataforma a través de credenciales.
2. Tener acceso a la solución de la plataforma de gestión y reportes a través de SSH desde el computador. Ingresar a la plataforma a través de credenciales.
3. Al ingresar las credenciales se debe observar un dashboard que contenga estadísticas de consumo del equipo FIREWALL.
4. Tener acceso via CLI (Command Line Interface) al o los equipos FIREWALL, través de la solución de gestión y reportes.
5. La solución debe permitir crear diferentes perfiles de usuario, administrando los privilegios y el acceso.
6. La solución debe permitir funcionalidades de auditoría para cada acción que realice dentro de una sesión un usuario.
7. La solución debe permitir crear al menos diez (10) usuarios con cualquiera de los siguientes perfiles:

PERFIL	PROPÓSITO
Administrador	Los usuarios a los que se les asigne este perfil deben estar en capacidad de ejecutar cualquier modificación sobre la plataforma, así como obtener información de configuración y desempeño de ésta.
Operador	Este tipo de usuarios pueden crear/modificar/eliminar usuarios sobre la plataforma que tengan el mismo perfil (operador), así como obtener información de configuración y desempeño de la plataforma.

8. Deben acceder vía HTTPS los diez (10) usuarios de manera concurrente a la plataforma de gestión y reportes.

Resultados prueba de validación	**Cumple** ☐	**No Cumple** ☐	**No verificado** ☐
Comentarios	• (Se debe escribir los comentarios relevantes a la prueba específica, si se presentaron inconvenientes, si faltaron recursos, problemas en las configuraciones, demoras y sus causas etc.….)		
Responsables:	**Proveedor:** **Firma** _____	**ETB:** **Firma** _____	

1.3.3. Gestión de logs y reportes

Ítem	Logs y reportes
Propósito	Verificar la gestión de logs y generación de reportes que se requieren para el servicio de ETB.

Ambiente de prueba:

Procedimiento:

1. Configurar el ambiente de prueba con el equipo FIREWALL en línea, de tal manera el tráfico hacia internet del computador cruce a través de el.
2. Conectar el equipo FIREWALL a la red de pruebas.
3. Conectar la plataforma de gestión y de reportes a la red de pruebas.
4. Configurar la red de pruebas para lograr los resultados esperados.
   a. Switching
   b. Routing
   c. SNMP Server
   d. NTP Server
5. Realizar las configuraciones necesarias en el equipo FIREWALL y en la plataforma de gestión y reportes.

Resultados esperados:

1. Evidenciar en la solución de la plataforma de gestión y reportes, estadísticas y graficas de la operación (CPU, RAM, etc) y funcionalidades del equipo FIREWALL.
2. Generar los siguientes reportes del equipo FIREWALL relacionados con:
   a. Reglas de Firewall Perimetral
   b. IDS/IPS
   c. VPN SSL e IPSec
   d. Antivirus
   e. Reporte de desempeño equipo FIREWALL: CPU, Memoria, Trafico por interfaces.
3. Los logs generados por la solución deben contener como mínimo, los campos listados a continuación:
   a. Identificador del elemento que genera el mensaje de log: puede ser dirección IP, nombre del dispositivo, etc.
   b. Fecha en la que se genera el mensaje
   c. Hora en la que se genera el mensaje
   d. Nivel de criticidad del mensaje
   e. Información del mensaje
4. Evidenciar que la solución de gestión y reportes genere y guarde los logs relacionados con el acceso de usuarios de administración y operación. Como mínimo estos logs deberán tener los campos indicados a continuación:
   a. Fecha en la que se genera el mensaje log
   b. Hora en la que se genera el mensaje
   c. Identificador del usuario para el cual se genera el mensaje log
   d. Acciones ejecutadas sobre la solución

Resultados prueba de validación	**Cumple** ☐	**No Cumple** ☐	**No verificado** ☐
Comentarios	• (Se debe escribir los comentarios relevantes a la prueba específica, si se presentaron inconvenientes, si faltaron recursos, problemas en las configuraciones, demoras y sus causas etc.….)		
Responsables:	**Proveedor:** **Firma** _____	**ETB:** **Firma** _____	

2. Pruebas de integración

2.1. Equipos firewalls nuevos

2.1.1. Pruebas de integración SNMP

Ítem	Pruebas de integración con SNMP V2c y V3		
Propósito	Verificar la integración de los equipos con la versión 2c y V3 de SNMP		
Ambiente de prueba:			
Procedimiento: 1. Habilitar SNMP V3 en el equipo firewall 2. Integrar el equipo firewall con el servidor SNMP de pruebas.			
Resultados esperados: 1. Verificación de los eventos de SNMP e integración con la V2c y V3 de SNMP.			
Resultados prueba de validación	**Cumple** ☐	**No Cumple** ☐	**No verificado** ☐
Comentarios	• (Se debe escribir los comentarios relevantes a la prueba específica, si se presentaron inconvenientes, si faltaron recursos, problemas en las configuraciones, demoras y sus causas etc.….)		
Responsables:	**Proveedor:** **Firma** _____	**ETB:** **Firma** _____	

2.2. Equipos Firewalls Fortinet

2.3. Sistema de gestión centralizada y reportes

3. Pruebas de procedimiento

3.1. Equipos firewalls nuevos

3.2. Equipos Firewalls Fortinet

3.3. Sistema de gestión centralizada y reportes

CONFIGURACIONES DEL EQUIPO
Si aplica. Utilizar letra Courier new o Lucida Consolé

RECURSOS UTILIZADOS
Lista de recursos empleados en las pruebas tales como: equipos, licencias, etc.

CONCLUSIONES Y RECOMENDACIONES FINALES

CONCLUSIONES:

- Se probó….
- Se encontraron dificultades……
- Todas las pruebas se hicieron con…….
- El resultado cumple con el RFC…
- Los índices medidos aplican dentro del rango según recomendación UIT o IEEE xxx o FOURUM xx.

RECOMENDACIONES:

- Lecciones aprendidas, comentarios para la mejora
- (Se hacen los comentarios relevantes a todo el proyecto, inconvenientes a tener en cuenta para agilizar una futura implementación, etc.….)
- Comentarios presupuestales si aplican
- Aplicación de mejores prácticas.

Los anexos en general nos permiten diseñar las plantillas para determinados servicios o productos validados

Anexo 1
(Tablas de resultados / logs). Utilizar letra Courier new o Lucida Consolé

Anexo 2
(Estadísticas y/o gráficos de pruebas)

Versión	Descripción del Cambio	Fecha del Cambio
1.0	Documento inicial	22/08/2017