**PLAN DE IMPLEMENTACION**

**Arquitectura General de la solución**

Con el contrato del cambio de los enlaces el mismo incluye el rubro de un firewall de borde mismo que servirá para llevar las reglas de la navegación y acceso a internet de la Cooperativa 29 de Octubre se requiere el poner en producción el equipo de firewall de borde.

**Propósito del cambio**

Separar las políticas de administración de internet “navegabilidad” del firewall perimetral Chekpoint para que se pueda administrar desde el firewall de borde Fortigate y así llevar por separada la administración de internet y puertos.

**Cronograma de Implementacion Propuesto**

Responsables

Cooperativa: Omar Redroban

Proveedor: Andres Noboa

Horario de trabajo

Sábado 20 de julio a las 17:00

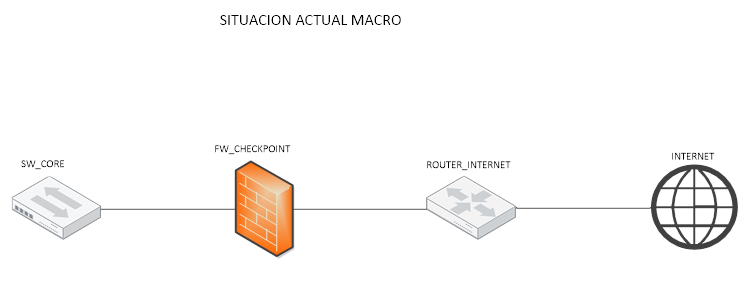
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Implementación** | **Responsable** | **Horas** | **Días** | **D1** |
| Colocación del equipo en un rack | Andres Noboa / Omar Redroban | 3:00 | 1 día |  |

La instalación se realizara según se indica el cronograma

|  |  |  |  |
| --- | --- | --- | --- |
| **Equipos** | **Hora Inicio** | **Hora Fin** | **Fecha** |
| Conexión del equipo al switch de core | 17:00 | 17:15 | 20/07/2019 |
| Verificar conectividad | 17:15 | 17:30 | 20/07/2019 |
| Activar Politicas configuradas en nuevo firewall | 17:30 | 18:30 | 20/07/2019 |
| Desactivar políticas de navegabilidad de Firewall Checkpoint | 18:30 | 19:00 | 20/07/2019 |
| Pruebas de navegabilidad desde firewall | 19:00 | 20:00 | 20/07/2019 |

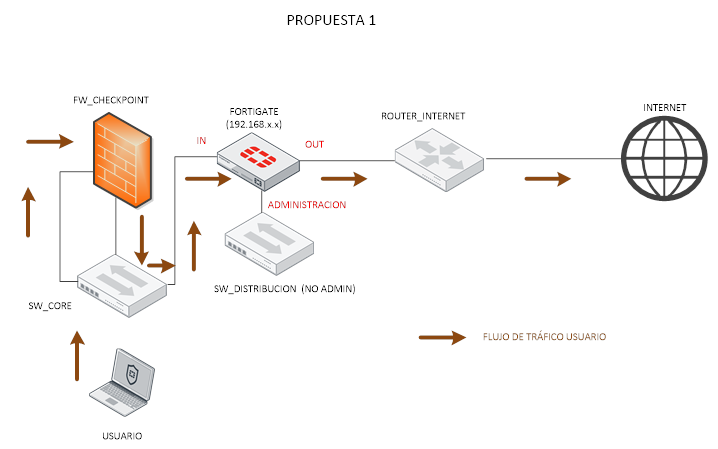
**Plan de implementación**

Situación actual de la cooperativa



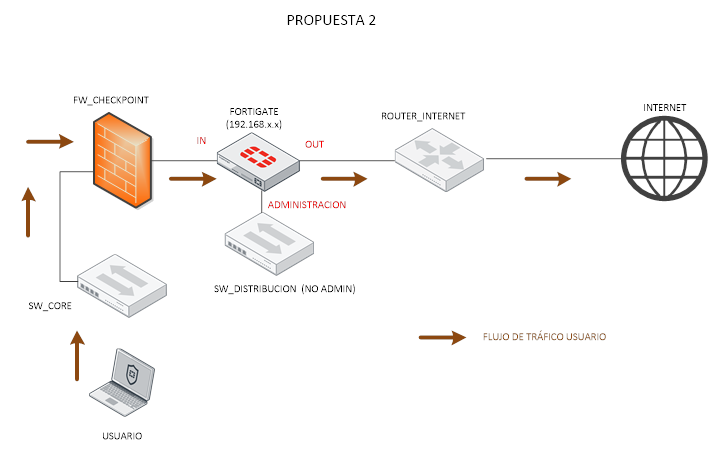
A continuación, se detallan los esquemas que se podrían aplicar para el cambio indicado:

1. Pasando por el switch de core 29 de Octubre. - Este esquema es el más recomendado ya que se puede partir asignando un puerto y probando conectividad de la IP mencionada en la parte superior hacia el AD, de tal manera que se pueda alcanzar por el vdom transparente los 3 ADs que tiene en la cooperativa. Para esto:



* 1. Se configura remotamente la IP en el Fortigate (vdom transparente).
  2. Se conecta el puerto asignado para IN de tráfico (puerto 11 de Fortigate) al switch de core. No existe afectación a menos que la IP esté duplicada.
  3. Una vez se configure el firewall y se autorice la ventana de puesta en producción, se debe por medio de configuraciones de capa 2 dejar pasar todo el tráfico por el esquema indicado a continuación, se activan las políticas del firewall de borde
  4. Se desactiva el control en el checkpoint, y el servicio quedaría migrado.
  5. Tener en cuenta que la interfaz OUT del firewall debe estar conectada a los routers de internet.

1. En la misma ventana de puesta a producción conectar directamente el Fortigate al equipo checkpoint (Asegurándose que la configuración de los puertos esté con parámetros de negociación automática), de tal manera que se mantenga la conexión mostrada a continuación:



* 1. Se ejecuta el mismo proceso que en la alternativa 1 con la diferencia que no se pueden ejecutar actividades previas.

Como pueden observar la criticidad se centra en la forma que se vayan a conectar los equipos ya que el firewall Fortigate al estar en modo transparente no tendrá direccionamiento (más que de administración para llegar al AD), rutas, nateos, etc. Toda la inteligencia la seguirán manejando los equipos de CHECKPOINT.

**Plan de Rollback**

En caso de existir algún problema la configuración debe quedar como se muestra en la gráfica de la situación actual