Documento de requerimientos

Sistema de comunicaciones seguras con segmentación virtual de dominios

Alberto Daniel Lange

26 de febrero de 2025

Resumen

Este documento es una descripción, basada en el método Arcadia, de los requerimientos de usuario del sistema completo. Se describe que necesita el sistema para cumplir las necesidades de los usuarios, las cuales son analizadas en el concepto de operaciones del proyecto. La solución propuesta para cumplir los requerimientos no se detallan aquí, sino en el documento de arquitectura.

v1.0

Índice

1 Requerimientos

1.1 Requerimientos funcionales

- **Renovación de claves:** cada par de nodos realiza una renovación de claves efímeras cada 120 segundos para asegurar forward-secrecy. Esto significa que, si una clave es comprometida por alguna razón, no se comprometen las comunicaciones anteriores o futuras fuera del intervalo de tiempo especificado.
- **Seguridad ante intrusiones:** el equipo debe ser capaz de mitigar la posibilidad de intrusiones de agentes no autorizados vía software, tanto desde Internet o como desde la red local.
- **Detección de ataques DoS:** el sistema debe ser capaz de detectar y mitigar ataques de denegación de servicio.
- **Movilidad:** el sistema debe ser capaz de soportar la movilidad de los nodos y permitir a un nodo moverse entre redes sin interrupciones ni renegociaciones de claves.
- **Split-tunneling:** el sistema debe ser capaz de permitir y enrutar tráfico de ciertas aplicaciones o servicios por fuera del túnel VPN.
- **Segmentación de dominios:** el sistema debe aislar procesos contenidos en un dominio de información, como pueden ser archivos, contenida en otro dominio, independientemente de los privilegios que tenga este proceso.

1.2 Requerimientos de rendimiento

- **Tasa de transferencia:** el sistema debe ser capaz de lograr, de un nodo a otro, una tasa de transferencia de 950 Mbits/s de datos planos.
- **Número de nodos:** una red segura debe ser capaz de soportar hasta 250 dispositivos encriptadores, también denominados nodos.

1.3 Requerimientos de interfaz

- **Administración:** la configuración de funcionamiento del encriptador debe poder ser modificada únicamente por un administrador de red autorizado de manera local.
- **Interfaz de usuario:** el sistema debe ser transparente para el usuario final, es decir, no debe requerir de configuraciones adicionales para este.
- **Configuración de operación:** el modo de operación en red del sistema y otros parámetros de funcionamiento asociados deben ser configurables únicamente por el administrador de red.