PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIÓNES

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGÍSTER EN REDES DE COMUNICACIÓNES

TEMA:

"ANÁLISIS Y MEJORA DE LA SEGURIDAD DE LA RED INALÁMBRICA BASADA EN W.I.P.S. Y PROPUESTA DE INTEGRACIÓN CON POLÍTICAS BASADAS EN BYOD (BRING YOUR OWN DEVICE): CASO DE ESTUDIO RED INALÁMBRICA DEL SERVICIO DE RENTAS INTERNAS QUITO AGENCIA PRINCIPAL".

DANIEL MAURICIO GARCÍA ZAPATA

Quito, Marzo 2017

DEDICATORIA

El presente, es el resultado de un trabajo en equipo que requirió tiempo, sacrificio y mucho apoyo, por ello, te dedico este trabajo a ti Valeria, mi esposa y compañera de vida que has estado apoyándome hoy como en innumerables ocasiones y tu amor y tu alegría ha sido siempre mi inspiración para seguir adelante.

Daniel García.

AGRADECIMIENTOS

"Educar es más difícil que enseñar, porque para enseñar se precisa saber, pero para educar se precisa ser". Quino.

Con esta frase, quiero iniciar agradeciendo a Dios por ser guía en mi camino y por darme la fortaleza para superar las adversidades que se me han presentado.

Muchas gracias a mis padres, Genaro y Piedad, porque en cada momento de mi vida estuvieron pendientes de mi formación como ser humano y gracias a ustedes tengo la mejor herencia, mi educación.

Gracias también a Eduardo y Patricio, mis hermanos, que con el paso del tiempo me han permitido aprender de ustedes y han sido mi ejemplo y su sola presencia ha sido un aliciente para mí.

Agradezco también a Vicente y Gioconda, por sus gestos de apoyo incondicional y desinteresado.

Finalizo mi agradecimiento y lo hago de manera muy sentida dirigiéndolo a la Pontificia Universidad Católica del Ecuador que me abrió sus puertas y me permitió culminar ésta etapa académica de mi vida y a cada uno de los integrantes del grupo de profesionales con los que tuve el gusto de contar, Ing. Juan Francisco Chafla, Ing. Francisco Rodríguez e Ing. Carlos Egas, a ustedes estimados docentes, muchas gracias por enriquecer el presente trabajo con sus acertadas contribuciones.

Daniel García.

RESUMEN

El crecimiento exponencial del uso de dispositivos móviles así como la gran demanda de acceso a internet, han fundado nuevas tendencias que han trascendido no solo al ámbito de la sociedad y su automatismo, sino también al ámbito laboral o empresarial, llevando a este último a enfrentar nuevos retos para garantizar la seguridad desde aspectos críticos como disponibilidad, confidencialidad e integridad de su información como su activo más valioso.

Las marcas líderes a nivel mundial han realizado aportes muy significativos en soluciones integrales de movilidad y seguridad, dando como resultado el desarrollo de tecnologías, herramientas y plataformas muy completas; muestra de ello es la tecnología Wireless Intrusion Prevention System que complementa a los esquemas de seguridad tradicionales en redes IEEE 802.11 proporcionando proactividad para detectar y evitar accesos no autorizados realizados con herramientas *open source* y mecanismos no estandarizados.

En este mismo contexto, la movilidad, ha obligado a adoptar tendencias empresariales en donde el protagonista es el empleado, el mismo que propone generar mayor productividad para la empresa al disponer de su propia tecnología al servicio de sí mismo y de sus actividades laborales.

Por lo expuesto, se cree pertinente, por una parte contar con una mejora que complemente el esquema de seguridad actual en la infraestructura inalámbrica de la "Empresa Pública de Recaudación de Impuestos" aplicando configuraciones adecuadas en los puntos críticos de dicha infraestructura que manejan la tecnología WIPS y además proponiendo una política basada en la tendencia BYOD que espera dejar el precedente para adoptar la misma a futuro.

ABSTRACT

The exponential growth in the usage of mobile devices as well as the high demand for Internet access, have founded new trends that have transcended not only the scope of society and its automatism, but also the workplace or business, leading the later to face new challenges in order to ensure security from critical issues such as availability, confidentiality and integrity of your information as your most valuable asset.

The worldwide leading brands have made significant contributions to comprehensive mobility and security solutions, resulting in the development of very complete technologies, tools and platforms. A proof of this is the Wireless Intrusion Prevention System that complements traditional security schemes in IEEE 802.11 networks providing proactivity to detect and prevent unauthorized access made with open source tools and non-standardized mechanisms.

In this context, mobility has forced the work style to adopt business trends where the protagonist is the employee, and hence it generates greater productivity for the company by having its own technology at the service of the employee and his or her work activities.

Therefore, it is considered relevant, on the one hand, to have an improvement that complements the current security scheme in the wireless infrastructure of the "Public Company of Tax Collection" applying suitable configurations in the critical points of that infrastructure that handle the WIPS technology. And on the other hand, to propose a policy based on the BYOD trend trying to leave the precedent to adopt it in the future.

ÍNDICE DE CONTENIDO

DEDICATORIA I

AGRADECIMIENTOS II

RESUMEN III

ABSTRACT IV

ÍNDICE DE CONTENIDO V

ÍNDICE DE FIGURAS VII

ÍNDICE DE TABLAS IX

1 CAPITULO I 1

1.1 INTRODUCCIÓN 1
1.2 JUSTIFICACIÓN 2
1.3 ANTECEDENTES 6
1.4 OBJETIVOS 11
1.4.1 Objetivo General *11*
1.4.2 Objetivos Específicos: *11*

2 CAPITULO II: MARCO TEÓRICO 12

2.1 ANTECEDENTES 12
2.2 ESQUEMAS DE SEGURIDAD EN REDES 16
2.2.1 Defensa en Profundidad y Seguridad Perimetral *18*
2.2.1.1 Firewall 21
2.2.1.2 Intrusion Detection System 24
2.2.1.3 Intrusion Prevention System 29
2.2.1.3.1 Arquitectura IPS 31
2.2.1.4 IPS según el Cuadrante Mágico de Gartner 32
2.3 SEGURIDAD EN REDES 802.11 34
2.3.1 Arquitectura de las redes 802.11 ..... *36*
2.3.2 Autenticación y Asociación en redes 802.11 ..... *38*
2.3.3 Mecanismos de seguridad en el estándar 802.11 ..... *40*
2.3.3.1 Wired-Equivalent Privacy – WEP 41
2.3.3.2 WPA / WPA2 43
2.3.3.3 Estándar de seguridad IEEE 802.11i 45
2.3.3.4 Estándar 802.1x 47
2.4 RIESGOS Y AMENAZAS FRECUENTES EN REDES 802.11 49
2.4.1 Vulnerabilidades de protocolos 802.11 ..... *49*
2.4.2 Ataques a redes 802.11 ..... *51*
2.4.2.1 Acceso no autorizado a la red. 52
2.4.2.2 Ataque “Man in the Middle” 54
2.4.2.3 Denial of Service - DoS 55
2.5 WIRELESS INTRUSION PREVENTION SYSTEM (WIPS) 57
2.5.1 Arquitectura de WIPS. *58*
2.5.1.1 Servidor WIPS. 59
2.5.1.2 Consola de administración WIPS. 60
2.5.1.3 Sensor inalámbrico WIPS. 60
2.5.2 Detección y prevención de Intrusos *61*
2.5.3 Monitoreo y Alertas. *63*

2.6 BRING YOUR OWN DEVICE 65
2.6.1 Ventajas y Desventajas 68
2.6.2 Mobile Device Management 70
2.6.3 Políticas BYOD 72
2.6.4 CISCO y BYOD 74
2.6.4.1 Cisco Identity Service Engine 75

3 CAPITULO III: DETERMINACIÓN DE SITUACIÓN ACTUAL RED INALAMBRICA SRI BASADA EN WIPS Y PROPUESTA DE MEJORA. 79

3.1 DESCRIPCIÓN DE LA "EMPRESA PÚBLICA DE RECAUDACIÓN DE IMPUESTOS". 79
3.2 ANÁLISIS SITUACIÓN ACTUAL (CONFIDENCIALIDAD) 81
3.2.1 Arquitectura de la Red Inalámbrica Institucional 82
3.2.1.1 Cisco Prime Infrastructure 84
3.2.1.2 Cisco MSE - Mobility Service Engine 86
3.2.1.3 Cisco Identity Service Engine 88
3.2.1.4 Wireless Lan Controller 89
3.2.1.5 Access Points 90
3.2.2 Esquemas de seguridad implementados en la red Inalámbrica 92
3.2.2.1 SSID para usuarios internos y externos. 92
3.2.2.2 WIPS en la "Empresa Pública de Recaudación de Impuestos" 97
3.3 PROPUESTA DE MEJORA 102
3.3.1 Configuración propuesta para Access Points 102
3.3.1 Configuración propuesta para Cisco MSE – Cisco Prime Infrastructure 106

4 CAPÍTULO IV: PROPUESTA DE POLÍTICA BYOD PARA DISPOSITIVOS MÓVILES 115

4.1 PROPUESTA DE POLÍTICA BYOD 115
4.1.1 Capa Operacional 116
4.1.1.1 On-boarding Policy. 116
4.1.2 Capa Táctica 118
4.1.2.1 Política de Control de Acceso e Identidad. 118
4.1.2.2 Política de Control de Riesgo. 119
4.1.3 Capa Estratégica 121
4.1.3.1 Política de Mantenimiento. 121

5 CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES 122

5.1 CONCLUSIONES 122
5.2 RECOMENDACIONES 124

6 BIBLIOGRAFÍA 127

7 ANEXOS 132

ÍNDICE DE FIGURAS

Figura 1. CIA triad - Triangulo CIA 14
Figura 2: Tendencias Cumbre de Seguridad y Gestión de Riesgos según Gartner..... 18
Figura 3. Capas de la arquitectura defense in depth. 20
Figura 4. Elementos de un esquema de seguridad perimetral empresarial. 21
Figura 5. Esquema de funcionamiento de un Firewall en una infraestructura corporativa 22
Figura 6. Filtrado por estado de paquetes ó stateful packet filtering. 24
Figura 8. Clasificación de IDS's más utilizados. 28
Figura 9: IPS/ IDS en modo in-line ubicado como punto de inspección y filtrado. 31
Figura 10: Arquitectura de un IDS / IPS. 32
Figura 11. Cuadrante Mágico de Gartner para IPS a noviembre 2015. 33
Figura 12. Ejemplo de WLAN basada en infraestructura. 37
Figura 13. Ejemplo de WLAN basada en ad-hoc. 37
Figura 14: Proceso de autenticación y asociación en un entorno 802.11 39
Figura 14: Estándares IEEE 802.11 más comunes. 41
Figura 15: Entorno corporativo 802.11. 52
Figura 16. Ataque mediante Rogue AP en entorno inalámbrico corporativo. 53
Figura 17. Ataque MITM utilizando evil twin AP. 55
Figura 18. Arquitectura solución basada en Wireless Intrussion Prevention System 59
Figura 19. Ejemplo Modulo CISCO WSM AIR-RM3000M 61
Figura 20. Metodologías de detección de Intrusiones. 63
Figura 21. Proyección de conectividad de dispositivos móviles para el 2017. 66
Figura 22. Esquema BYOD ejemplo para infraestructura inalámbrica. 69
Figura 23. Arquitectura de política BYOD. 74
Figura 24. Arquitectura de componentes de Cisco ISE. 76
Figura 25. Proceso de On-boarding mediante Cisco ISE y SSID simple. 77
Figura 26. Diagrama topológico principales componentes infraestructura. 83
Figura 27. Arquitectura Red Inalámbrica Institucional. 84
Figura 28. Cisco MSE. 87
Figura 29. Interfaz WLC primario. 89
Figura 30. Configuración General SSID "FUNCIONARIOS" 93
Figura 31. Configuración seguridad capa 2 SSID "FUNCIONARIOS" 94
Figura 32. configuración RADIUS SSID "FUNCIONARIOS" 94
Figura 33. Configuración General SSID "SRI_CIUDADANO" 95
Figura 34. Configuración seguridad capa 2 SSID "SRI_CIUDADANO" 96
Figura 35. Validación de módulo WSM en AP Cisco 3700. 99
Figura 36. Validación de no disponibilidad módulo WSM en AP Cisco 3700. 99
Figura 37. Configuración AP con módulo WSM. 100
Figura 38. Perfiles WIPS. 101
Figura 39. Acceso a Access Points desde Cisco Prime Infrastructure. 104
Figura 40. Access points con modulo WSM. 104
Figura 41. Desactivación temporal Admin status. 105
Figura 42. Activación modo FlexConnect y sub-modo wIPS. 106
Figura 43. Acceso a configuración de perfiles wIPS. 107
Figura 44. Perfiles wIPS creados 108

Figura 45. SSID Group List creado para perfil wIPS. 108
Figura 46. Categorías de seguridad predefinidas dentro de perfil wIPS creado. 109
Figura 47. Categorías de seguridad DoS Attack Against AP. 110
Figura 48. Configuración politica DoS Association flood. 112
Figura 49. Configuración politica DoS MDK3-Destruction attack. 113
Figura 50. Configuración política DoS Probe response flood. 113
Figura 51. Configuración política Spoofed MAC address detected. 114
Figura 52. Arquitectura de Política BYOD propuesta. 116

ÍNDICE DE TABLAS

Tabla 1. Resumen de tipo de seguridad y Mecanismo de cifrado para WPA y WPA2. 45
Tabla 2. Principales opciones de seguridad para las redes 802.11. 47
Tabla 3. Tipos de ataques DoS. 56
Tabla 4. Posibles amenazas inalámbricas detectables por IDS/IPS. 64
Tabla 5. Consideraciones y criterios específicos para una política BYOD. 73
Tabla 6. Cantidad de AP's por modelo "Empresa Pública de Recaudación de Impuestos" 90
Tabla 7. Distribución Módulos WSM "Empresa Pública de Recaudación de Impuestos" 91
Tabla 8. Access Points con módulo WSM. 100
Tabla 9. Principales puertos de servicios utilizados por BYOD con Cisco ISE. 120

1 CAPITULO I

1.1 Introducción

El presente trabajo presenta los parámetros más relevantes de seguridad que se maneja en una red inalámbrica que utiliza la tecnología WIPS (wireless intrusion prevention system) y que es susceptible de mejora mediante la optimización de su infraestructura inalámbrica instalada. El principal objetivo es analizar la seguridad que puede brindar dicha tecnología a una red WLAN que provee conectividad mediante el estándar 802.11 en una institución pública y proponer una política con base a la tendencia empresarial BYOD (bring your own device) para realizar una gestión completa de los dispositivos móviles que utilizan los servicios de esta infraestructura.

Con este trabajo se pretende ofrecer una perspectiva concreta acerca de las funcionalidades y las ventajas que supone la utilización de la tecnología WIPS para prevenir ataques maliciosos y garantizar la integridad de la red inalámbrica de una empresa pública o privada y por otra parte pretende revisar soluciones y mejores prácticas que complementen y exploten las funcionalidades que brinda dicha tecnología.

Aunque actualmente existen sistemas basados en hardware y software dedicados a detectar o prevenir ataques o intrusiones no autorizadas, en su mayoría se enfocan en brindar seguridad en redes cableadas, son pocas las soluciones integrales que proveen seguridad a las redes inalámbricas y peor aún no existe alguna documentación sobre los procedimientos que le permita a la empresa manejar un escenario en el cual deba brindar conectividad inalámbrica a los dispositivos móviles propios o de personas externas a la institución.

En este contexto el presente trabajo procura, esencialmente y en primer lugar analizar el nivel de seguridad que puede proveer la tecnología WIPS y proponer posibles mejoras que

garanticen un funcionamiento continuo en la red inalámbrica y de manera consecuente, que en el caso que existan eventos en donde se vea comprometida la seguridad, integridad o confidencialidad de la red, se tomen acciones de manera automática. En segundo lugar se pretende plantear una política que cuente con los lineamientos básicos para regular el uso de los dispositivos móviles de la institución o de los empleados enmarcados en el contexto de la seguridad de la información.

En este contexto, en este primer capítulo se muestra brevemente algunos de los trabajos previos realizados y que le atañe relación con el tema. Posteriormente se plantean los argumentos que justifican su desarrollarlo y finalmente se muestran los objetivos como elementos indispensables que dan la pauta al desarrollo de la investigación.

1.2 Justificación

Desde la estandarización de las redes inalámbricas que de acuerdo a (Chandramouli, 2002) fue en el año 1997 y su uso a lo largo del tiempo, ha sido notoria la universalidad con la cual se han posicionado las comunicaciones inalámbricas en distintos escenarios como hogares, campus universitarios, parques hasta grandes empresas con distintas sucursales. Comenzando en implementaciones caseras hasta grandes proyectos que cubren distancias geográficas extensas que antes no podían ser imaginadas, son prueba que confirman la gran evolución que este tipo de redes ha tenido y a su vez dejan clara la importancia que tienen para nuestras vidas, pues este tipo de redes proveen una amplia gama de ventajas como su instalación, cobertura, escalabilidad y sobre todo movilidad, siendo hoy por hoy casi concluyente el hecho de que cualquier individuo con un dispositivo móvil pueda captar la

señal de un equipo que brinda conectividad mediante el estándar 802.11 que define a las redes LAN inalámbricas.

Con la misma celeridad se ha notado la meticulosa transición que se ha dado en ciertos escenarios desde las redes cableadas hacia las redes inalámbricas así como según (López, 2015) se ha incrementado de manera exponencial el nivel de penetración de los dispositivos móviles en todos los ámbitos de la vida cotidiana según estudios realizados recientemente por la empresa eMarketer a nivel de Latino América, lo que involucra una mayor demanda de conectividad inalámbrica así como los aspectos e implicaciones de seguridad que deben cubrir las empresas que implementen o tengan implementado este tipo de redes, pues de manera intrínseca una red inalámbrica es insegura y está expuesta a amenazas y ataques que hoy por hoy son tan comunes como por ejemplo la obtención ilegal de claves, intrusiones no autorizadas e incluso la denegación de servicio denominado DoS, entre otras.

Consecuentemente, gran parte de las empresas públicas y privadas en el Ecuador han adoptado a las redes inalámbricas como opción de conectividad, sobre todo por aspectos económicos, geográficos y técnicos, sin embargo es sumamente importante considerar que el "aire" como medio de comunicación o guía de onda de una red inalámbrica es un medio muy vulnerable e inestable y para ello cada estándar de la familia 802.11 implementa ciertos mecanismos para garantizar disponibilidad, fiabilidad y sobre todo seguridad en la comunicación.

La movilidad como una de las principales ventajas de las redes 802.11, se identifica a su vez como una vulnerabilidad desde el punto de vista del anonimato por cuanto es más complejo determinar quién intenta acceder sin autorización a una red WLAN; de ello se desprende que el objetivo final de implementar seguridad en una red, independientemente de su naturaleza es, entre otros aspectos, mantener control de acceso o evitar que ciertos intrusos puedan acceder a los recursos que dicha infraestructura pueda disponer sin ser detectados.

En este sentido existen mecanismos para asegurar la transmisión de información como por ejemplo encriptar la comunicación AP - ESTACIÓN, mediante el uso de protocolos básicos como WEP (wired equivalent privacy) o WPA (WI-FI protected access) para proveer un mínimo nivel de privacidad a la WLAN, sin embargo en entornos empresariales, se manejan arquitecturas de red inalámbricas que complementan su seguridad con el uso de protocolos más avanzados como WPA2 o WPA2 ENTERPRISE, servidores de autenticación RADIUS, firewall, AAA, IPS/IDS, entre otros.

Los sistemas de prevención/detección de intrusiones IPS/IDS son mecanismos más avanzados y complejos que evolucionaron para proveer seguridad también en redes inalámbricas previniendo o detectando el acceso no autorizado a una infraestructura de red por medio de monitoreo, recolección, análisis, alarmas, notificaciones y bloqueos. Estos a su vez, se ha constituido la primera línea de defensa en los actuales sistemas de seguridad perimetral y pueden ser implementados en soluciones hardware o software.

En este contexto la tecnología WIPS (wireless intrusión prevention system) integra las características de un IDS con la capacidad de tomar acciones correctivas en función de los análisis de datos realizados cuando existe actividad sospechosa en la red.

Las bondades que esta tecnología provee, permite integrarla fácilmente con las políticas empresariales para gestión y manejo adecuado de políticas, permisos y conexiones de dispositivos móviles propios o ajenos a la institución, lo que fácilmente permiten deducir que una de las mejores opciones para brindar seguridad a la red inalámbrica podría ser el uso de dicha tecnología considerando las prioridades de la empresa y una política que regule el uso y acceso a los servicios de dicha red.

Sin duda que únicamente el hardware instalado no constituye el todo de la seguridad de una red, detrás de ello se encuentra la gestión centralizada que principalmente se encuentra representada por software que denominado MDM por sus siglas en inglés Mobile Device Management que según refieren (Diogenes & Gilbert, 2015) en palabras sencillas es un conjunto de mecanismos para asegurar, controlar y administrar los dispositivos móviles que se conectan a la red inalámbrica.

Por otra parte, existe gran cantidad de trabajos relacionados con la seguridad física y lógica a nivel de redes cableadas e inalámbricas, sin embargo son pocos los trabajos relacionados al estudio del estado de arte de la tecnología WIPS y peor aun considerando que son pocas las marcas que manejan dicha tecnología y en su mayoría son tecnologías que son subutilizadas.

En conclusión la importancia de este proyecto reside por una parte en el uso y optimización de nuevas tecnologías de seguridad provistas como soluciones propietarias y probadas, para garantizar la seguridad de una red y su infraestructura y además facilitar su

gestión mediante la aplicación de políticas desarrolladas para su fin y por otra parte constituirse como un documento bibliográfico aplicable en la empresa pública considerando que hoy en día es necesario contar con la documentación necesaria para operar la tecnología que está implementada en dicho sector.

En este contexto, las nuevas tendencias empresariales conocidas como BYOD se constituyen en un factor que brinda mucha importancia al presente proyecto, por que dichas tendencias han trascendido en el ámbito empresarial así como en el ámbito técnico y permiten documentar y delimitar los procedimientos para que se justifique una adecuada manera de gestionar o manejar las conexiones de equipos móviles internos o externos y más aun considerando que actualmente no se cuenta con una política BYOD base para el usuario final.

1.3 Antecedentes

Aunque el estándar 802.11 no es reciente, ha evolucionado en sus distintas versiones así como en sus características y también han evolucionado los mecanismos con los cuales se puede mejorar la seguridad de una infraestructura tecnológica como servidores, técnicas de seguridad y potentes mecanismos de autenticación que juegan un papel sumamente importante para mantener la confidencialidad de una red WLAN y por ello empresas a nivel mundial han optado por implementarla considerándola como una herramienta para proveer facilidad de gestión , control centralizado, flexibilidad y a su vez mejorar la productividad de sus empleados.

En este contexto, esta alternativa ha significado un reto para los administradores TI por que los datos están siendo transmitidos vía ondas de radio y esto de por sí implica

vulnerabilidad en los entornos empresariales obligando a integrar diversas tecnologías con el objetivo de evitar accesos no autorizados a los recursos de la red.

Como antecedente legal, es muy importante mencionar que en el Ecuador, según los art. 229 – 234 del Código Orgánico Integral Penal COIP reformados por (Asamblea Nacional del Ecuador, 2014), se considera un delito informático desde la interceptación ilegal de datos hasta el acceso no consentido a un sistema informático, telemático o de telecomunicaciones. En España por ejemplo, el portal (Delitos Informaticos, 2015), indica que el 63.89% de los delitos informáticos están relacionados con acceso ilícito a sistemas informáticos. Estos datos toman relevancia cuando personas sin Ética o con algún interés utilizan equivocadamente la tecnología o se aprovechan de sus vulnerabilidades y acceden a los recursos de una infraestructura tecnológica a los cuales no están autorizados.

Los intentos por asegurar la confidencialidad de una red informática han permitido a los fabricantes desarrollar productos en Hardware y Software que integren principalmente la gestión centralizada de la red y la aplicación de políticas que garanticen el acceso únicamente a equipos autorizados, todo esto mediante una combinación entre ambientes web amigables con el usuario, sensores, analizadores de tráfico, técnicas de detección y prevención de intrusiones y las ventajas que la familia de estándares 802.11 permite.

Estas iniciativas han tomado importancia por las ventajas de integración, facilidad y seguridad que ofrecen, sobre todo en infraestructuras grandes con altos niveles de criticidad de la información, en donde mantener la confidencialidad es uno de los principales objetivos, en donde a pesar de contar con esquemas de seguridad tradicionales y no por ello menos seguros, se necesita proveer de seguridades adicionales. Sin duda que la implementación de firewall, IPS/IDS, servidores de autenticación y demás mecanismos de seguridad disminuyen la posibilidad de acceso no autorizado; sin embargo y como se ha

mencionado anteriormente los métodos de intrusión también son objeto de mejora, por lo cual se hace necesario innovar con tecnologías más complejas como por ejemplo Wireless Intrusion Detection System y políticas de gestión y manejo de dispositivos móviles.

La tecnología WIPS o wireless IPS como también se lo denomina y como una evolución de IDS, forma parte del tema de investigación del presente proyecto de tesis y aunque fue oficializado en el año 2009 no se sabe con certeza las instituciones que manejan su infraestructura de red en base a esta tecnología en el Ecuador. Las principales marcas proveen productos con tecnología WIPS como lo menciona (CISCO, 2014) que refiere su solución Cisco wIPS, (MOTOROLA, 2011) en cambio refiere su solución AirDefense, (HP, 2010) refiere su solución AirProtect Wireless Security Series y dicho sea de paso estas marcas garantizan su funcionamiento y soporte lo que las hace más atractivas para el sector empresarial cuando se trata de implementar soluciones o innovarlas.

Aunque las arquitecturas de seguridad en redes 802.11 manejan esquemas tradicionales en hardware y software como encriptación con claves WEP/WPA2, servidores de autenticación RADIUS, tecnología 802.1x, AAA, firewall, es importante la innovación considerando siempre aspectos como seguridad, economía y política pública. En este contexto es muy acertado recordar lo mencionado en párrafos anteriores y es que existen plataformas que apoyan y complementan la gestión centralizada de una infraestructura de red corporativa de manera amigable y sencilla que incluye distintos niveles de acceso.

Aunque en la actualidad existen herramientas “open source” destinadas a realizar un “ethical hacking” en el ámbito de las redes 802.11 como por ejemplo SNORT, con la finalidad de evaluar la seguridad de una red inalámbrica desde el punto de vista de un

IDS/IPS, se destaca que no son soluciones probadas que garanticen un nivel de estabilidad, disponibilidad o calidad de servicio, lo cual las hace muy poco apetecidas.

Pero no todo ha sido hardware y software, por cuanto un factor importante a la hora de gestionar la seguridad de una infraestructura tecnológica es la política que regule internamente dicha gestión. En este sentido otra temática de análisis en el presente proyecto de tesis es según (Wikipedia, 2016) la tendencia empresarial BYOD y su posibilidad de integración con las políticas de gestión de dispositivos móviles. El Ecuador ha ido adoptando dichas tendencias según estadísticas de (ESET, 2012) desde aproximadamente dos años.

Existen iniciativas que se originan principalmente en universidades y escuelas politécnicas y que para el presente proyecto de tesis constituye un antecedente bibliográfico y definitivamente un aporte significativo de contenido científico.

En la Escuela Politécnica Nacional por ejemplo, se han realizado algunos proyectos de tesis de pregrado referente a seguridades de la red y afines al presente proyecto; por ejemplo se menciona la tesis de pregrado de (Sánchez Prieto, 2012), en la cual se propone netamente el diseño de un sistema que permita garantizar la seguridad de la red LAN de una institución pública incluso mediante la implementación de políticas afines.

Por otra parte según (Guaño Aucancela & Novillo Ortega, 2012), en su tesis de pregrado proponen el diseño de un módulo de inteligencia artificial para que acoplado a un IDS pueda detectar posibles intrusiones no autorizadas en una red cableada.

Otro trabajo relevante es referido por (Balseca Guzmán, 2013) en donde se realiza un análisis exhaustivo sobre las principales características del estándar 802.11 y los mecanismos de seguridad con los que cuenta; adicionalmente se menciona a los WIDS sistemas de detección de intrusiones y sus técnicas de detección.

A nivel de artículos técnicos se han encontrado algunos aportes investigativos principalmente en la librería digital de IEEE que mencionan estudios sobre ciertas temáticas en particular dentro del ámbito de la tecnología Wireless IPS y para citar dos ejemplos, (Zhang , Chen , Wang , & Weng , 2010) menciona la evolución de los sistemas de prevención de intrusos y se plantea un framework común para la tecnología WIPS.

Por otra parte (Chen , Yao , & Wang , 2009)) mencionan desde las principales amenazas del estándar 802.11 hasta presentar un framework WIPS para obtener patrones de comportamiento de ataques mediante el uso de honeypots o equipos trampa.

Un artículo que contribuye de gran manera al presente proyecto de tesis, es de (Vanjale & Mane , 2015), en donde se expone varios aspectos importantes acerca de métodos para detectar rouge APs o puntos de acceso fantasma como mecanismo de prevención de acceso no autorizado.

A nivel de postgrado, en Ecuador, no se ha encontrado estudios a fines a la tendencia empresarial BYOD o algún trabajo investigativo que integre las temáticas de análisis declaradas en el presente proyecto de tesis, por lo cual, se hace necesaria la propuesta de un documento que le permita a la empresa que es objeto del presente caso de estudio, conocer los mecanismos para gestión de los dispositivos móviles en casos muy específicos

basados en su situación actual aprovechando la infraestructura instalada y que se considere la alternativa de mejorar dicha infraestructura para detectar intrusiones no autorizadas a su red inalámbrica.

1.4 Objetivos

1.4.1 Objetivo General

Analizar y mejorar la seguridad de una red inalámbrica basada en la tecnología W.I.P.S. con la posibilidad de integración con la tendencia empresarial BYOD tomando como caso de estudio la red inalámbrica del Servicio de Rentas Internas - agencia principal.

1.4.2 Objetivos Específicos:

1. Analizar las características de seguridad más relevantes del estándar IEEE 802.11 y WIPS para integrarlas con políticas BYOD.
2. Determinar la situación actual de la red inalámbrica del contribuyente del SRI basada en W.I.P.S. y propuesta de mejora.
3. Proponer una política B.Y.O.D. para dispositivos móviles orientándola al usuario interno del Servicio de Rentas Internas.

2 CAPITULO II: MARCO TEÓRICO

El contexto temporal y situacional del presente trabajo de tesis, se lleva a cabo en una institución pública dedicada a la administración tributaria a la cual se la denominará en adelante "Empresa Pública de Recaudación de Impuestos".

2.1 Antecedentes

"El único sistema realmente seguro es el que está apagado, dentro de un bloque de concreto y sellado en una habitación con plomo y con guardias armados – e incluso así, tengo mis dudas." (Dewdney, 1989)

El presente capítulo, inicia citando esta frase del PhD. Alexander Dewdney, que sin duda resulta desafiante suponer un entorno en el cual se garantice la seguridad de un sistema o red informática de la manera más retrograda considerando que el mundo actual desarrolla sus comunicaciones mediante la magnífica interacción entre distintos canales, producto de la utilización de dispositivos como computadores, smartphones y demás tecnología que garantiza un intercambio de información con otras personas geográficamente distantes.

En este contexto, no cabe duda que la seguridad informática ha evolucionado y es un aspecto que le atañe gran importancia al presente trabajo de titulación que más que todo se apoya en conceptos afines pero que en esencia se enfoca a los aspectos más relevantes de la seguridad en redes inalámbricas y sus plataformas comerciales más conocidas.

Para posicionar claramente al presente capítulo, es adecuado contrastar la idea de aislar un recurso informático para garantizar su seguridad versus la necesidad de interconectar dichos recursos implementando un conjunto de medidas que reduzcan las vulnerabilidades

a las que dichos recursos están expuestos pero sin que ello obstaculice la interacción del usuario final con la infraestructura tecnológica.

Cobra sentido entonces, comenzar definiendo ciertos conceptos afines al tema que permitirán entender de manera más adecuada el ámbito de la seguridad aplicada a aspectos informáticos por ejemplo una red de computadoras, según Migga (2009, pág. 3) la define como "un sistema distribuido que consiste en un acoplamiento flexible entre ordenadores y otros dispositivos".

Por otra parte, con la evolución de las redes y facilidades de comunicación así como con la trascendencia de los tradicionales sistemas de almacenamiento de información, fue evidente generar mecanismos o herramientas para protegerla contra el acceso no autorizado, por ello William Stallings define a la seguridad informática como "…el nombre genérico para la colección de herramientas diseñadas para proteger los datos y para frustrar a los hackers…". (2011, pág. 3)

Por otra parte, el NIST Computer Security Handbook en su sección de terminología importante define el término seguridad informática como "…la protección otorgada a un sistema de información para alcanzar los objetivos aplicables de preservar la integridad, disponibilidad y confidencialidad de los recursos del sistema de información (incluyen hardware, software, firmware, información/data y telecomunicaciones)…". (Guttman & Roback, 1995, pág. 5)

Complementando estas definiciones, se introducen los conceptos de confidencialidad, integridad y disponibilidad, tres conceptos claves que dan sentido a la seguridad informática y se definen mediante el "CIA triad" o "triángulo CIA", ver figura 1.

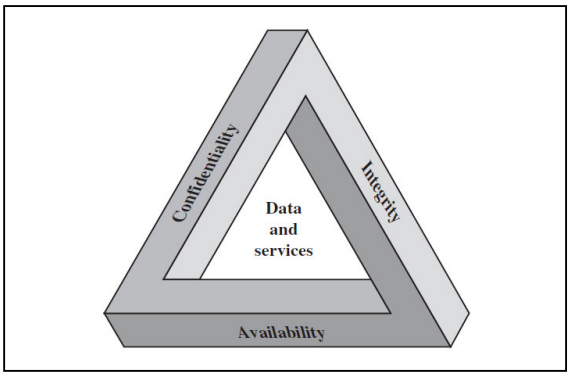


Figura 1. *CIA triad - Triangulo CIA*

Fuente: (Stallings, 2011, pág. 4)

En términos muy sencillos el triángulo CIA, se enfoca en los datos y en servicios de computación, así la confidencialidad restringe la divulgación no autorizada, la integridad garantiza la autenticidad y la disponibilidad asegura el acceso permanente a la información o a los servicios de computación.

Algunos expertos proponen la autenticidad y accountability o cumplimiento de responsabilidades como dos de los elementos más comúnmente mencionados para complementar los definidos en el triángulo CIA. La autenticidad busca certificar o verificar que los usuarios son quienes dicen ser y la accountability se enfoca en hacer un rastreo y registro de acciones realizadas por una entidad.

En publicaciones más recientes, Richard Brooks (2014, pág. 25) considera a esta perspectiva como tradicional y se profundizan en las propiedades que debería tener la disponibilidad de un sistema como factores importantes para la seguridad que se describen a continuación:

- Confiabilidad
- Disponibilidad
- Safety

- Tolerancia a Fallos
- Auto-estabilización

Los argumentos expuestos en párrafos anteriores, constituyen criterios muy importantes que permiten a los administradores de una red definir los mejores mecanismos para asegurar a sus recursos, hardware o software, sobre todo a su data, principalmente de accesos no autorizados interna y externamente.

Uno de los más importantes y actuales enfoques en seguridad de redes determina que para maximizar la seguridad de un recurso se debe tratar de aislarlo de ataques potenciales. Sin embargo esto no debe obstaculizar la posibilidad de un usuario para interactuar con los recursos de una red (Brooks, 2014, pág. 125). De este argumento se desprende la seguridad física y lógica como un aspecto que según Joseph Migga (2005, pág. 68), está garantizado solo si una infraestructura está cubierta por una barrera y cumple con cuatro mecanismos:

- Disuasión.
- Prevención.
- Detección.
- Respuesta.

Desde un punto de vista diferenciado, la seguridad física de una infraestructura tecnológica va estrechamente relacionada con la seguridad lógica o técnica pues si la seguridad física falla, los mecanismos de seguridad técnica podrían ser intervenidos fácilmente dando lugar a escenarios tan críticos como implementación de Rogue Ap's, sniffers, keyloggers, etc.

En este contexto, la necesidad de implementar seguridad física responde a razones que se justifican en la protección del activo más importante: la información y su infraestructura tecnológica, como se menciona anteriormente.

De acuerdo a esto, Kimberly Graves en el *Official Certified Ethical Hacker Review Guide* [CEH] (2007, pág. 197), categoriza las medidas de seguridad como físicas, técnicas y operacionales. En el contexto de la "Empresa Pública de Recaudación de Impuestos" en la cual se lleva a cabo el presente proyecto de tesis, se entenderá como seguridad técnica a las tecnologías y mecanismos basados en software o hardware utilizados para garantizar la seguridad de la infraestructura tecnológica y sus recursos de accesos no autorizados. Dentro de esta categorización se encuentran tecnologías de seguridad como firewalls, IDS's, IPS's y demás mecanismos complementarios.

2.2 Esquemas de seguridad en redes.

Históricamente, la seguridad de redes ha debido evolucionar considerando el incremento desmedido de tecnologías para administrarla así como los métodos maliciosos para evadirla. Esta evolución conllevó la concepción de estándares que permitan converger intentando cubrir la administración de la seguridad desde cinco perspectivas que son: administración de fallos, configuración, contabilidad, rendimiento y seguridad.

Organizaciones internacionales como IETF, IEEE, ISO, ITU, CEN, CEU, ETSI, NIST, ANSI, CSC, entre otras, han sido quienes han posibilitado dicha estandarización de la cual se debe resaltar el estándar ITU-T X.800 (Jacobs, 2014, pág. 15), que cubre la administración de la seguridad y sus recursos.

El estándar ITU-T X.800 o ISO/IEC 7498–2 como también se lo conoce, contempla la introducción y definición de cuatro parámetros como son:

- **Servicios de seguridad de Red**: Contempla Autenticación, Control de Acceso, Confidencialidad, Integridad y No Repudiación.
- **Conjunto de mecanismos específicos de seguridad de red**: Define cifrado, firmas digitales, mecanismos de control de acceso e integridad de la Data, entre otros.
- **Conjunto de mecanismos de seguridad para dispositivos no específicos**.
- **Mecanismos de administración para controlar mecanismos de seguridad implementados**.

En el contexto de los conceptos descritos en párrafos anteriores, la seguridad de una red corporativa está alineada con la utilización de mecanismos, servicios y sistemas de administración que permitan prevenir y minimizar los riesgos de acceso no autorizado. Por ello, en la actualidad los administradores de red de las organizaciones y grandes empresas independientemente del giro del negocio, implementan toda una infraestructura tecnológica en hardware y software para facilitar la gestión de su información por ejemplo mediante sistemas de información, consolas de administración, portales de gestión web, bases de datos, etc.

2.2.1 Defensa en Profundidad y Seguridad Perimetral

Como se había mencionado en el ítem anterior 2.1 Antecedentes, el crecimiento exponencial de las redes y los dispositivos finales en la última década entre ellos los smartphones, ha obligado a innovar a una gran velocidad los tradicionales métodos de seguridad de la red y llevarlos a otro nivel. Las tendencias que han marcado las estadísticas refieren que serán 20.8 Millones de dispositivos conectados para el año 2020 como sinónimo del IoT (Internet of Things) lo que generará un impacto de $11.1 Trillones de dólares como puede observarse en la figura 2.

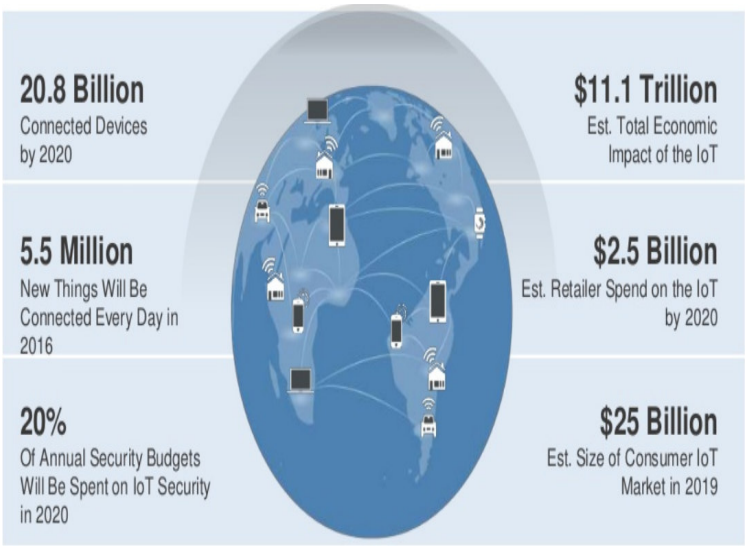


Figura 2: Tendencias Cumbre de Seguridad y Gestión de Riesgos según Gartner.

Fuente: (Rob MacDonald, Rebecca Golden, 2016, pág. 3)

En este mismo contexto, los administradores de red deben establecer un método de defensa que garantice la seguridad física y lógica de una red considerando dos contextos: seguridad en capas y seguridad en su borde o perímetro externo.

El término *defense in depth* se utiliza a menudo sin entender su concepto, sin embargo refiere la segmentación de la seguridad en distintos niveles o lo que textualmente significaría una seguridad en profundidad.

Muchos autores lo consideran como una arquitectura o estrategia de seguridad sin embargo otros la refieren como "una arquitectura de defensa bien estructurada que trata a la seguridad de la red como una cebolla" (Northcutt, Zeltser, Winters, Kent, & Ritchey, 2005, pág. 31).

Es evidente pensar que esta arquitectura de seguridad le dificulta al atacante la posibilidad de tener éxito en un intento de penetración, por cuanto cada capa garantiza el uso de buenas prácticas para mitigar dichos ataques.

En contraste con lo mencionado anteriormente, la arquitectura *defense in depth* consiste en:

- Directivas – Procedimientos.
- Seguridad Física.
- Seguridad Perimetral.
- Seguridad de Red Interna.
- Seguridad en Host.
- Seguridad en Aplicaciones.
- Seguridad de Datos.

La figura 3, muestra lo mencionado anteriormente.

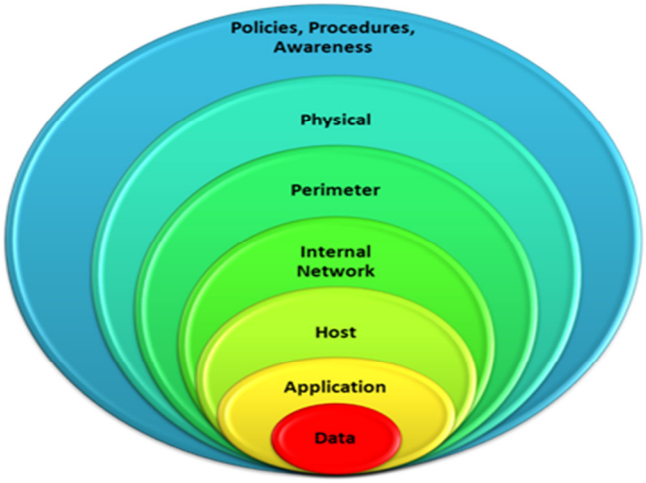


Figura 3. Capas de la arquitectura defense in depth.

Fuente*:* (Assee, 2011, pág. 7)

La seguridad perimetral como componente primordial de la defensa en profundidad, define el alcance y a su vez el límite lógico entre la red interna y otras redes mediante reglas o políticas para controlar a quienes están y no están autorizados a acceder a dicha red.

La seguridad perimetral según (Northcutt, Zeltser, Winters, Kent, & Ritchey, 2005) identifica a una área o zona fortificada de una red que puede contener elementos como; routers de borde, firewalls, IDSs, IPSs, DMSs, etc.

Es decir que los elementos mínimos para certificar seguridad en una red se los puede enumerar como se puede apreciar en la figura 4.

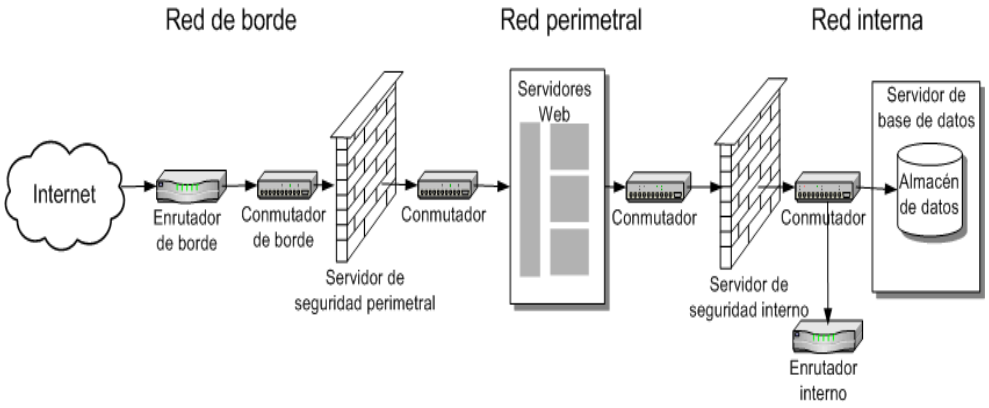


Figura 4. Elementos de un esquema de seguridad perimetral empresarial.

Fuente: (MICROSOFT CORPORATION, 2017)

2.2.1.1 Firewall

En el contexto de la seguridad en profundidad o defense in depth y la seguridad perimetral podemos destacar elementos tan críticos dentro de estos esquemas de seguridad como el firewall, los IPS e IDS.

Cuando se piensa en un firewall de manera casi textual se nos presenta una imagen de una *muralla de fuego* que sin duda da la idea de obstáculo, división, aseguramiento, protección, dificultad y otros sinónimos que en esencia denotan algún tipo de impedimento.

En ocasiones se concibe a un firewall como una simple caja con el propósito específico de controlar el tráfico de internet y aunque en cierta forma lo es, un firewall puede implementárselo como una función de un equipo de enrutamiento por ejemplo o como un sistema muy complejo, distribuido e interconectado que combina hardware y software para controlar o limitar el acceso a una red informática (Cheswick, Bellovin, & Rubin, 2003).

Migga (2015, pág. 249) define: "un firewall es un hardware, software o una combinación de ambos que monitorean y filtran tráfico de paquetes que intentan entrar o salir de la red privada protegida".

En una apreciación muy personal un firewall es un mecanismo de control que basado en políticas de seguridad realiza un filtrado de paquetes, aceptando o denegando su paso a través de él de una red hacia otra, evitando así el acceso no autorizado. Esto lo constituye como la primera línea de defensa de la red.

En un contexto corporativo, el firewall monitorea el intercambio de paquetes entre la red corporativa (red confiable) y la red externa internet (red no confiable) sin que esto impida la comunicación fluida entre equipos finales. Esta función puede observarse de manera más clara en la figura 5.

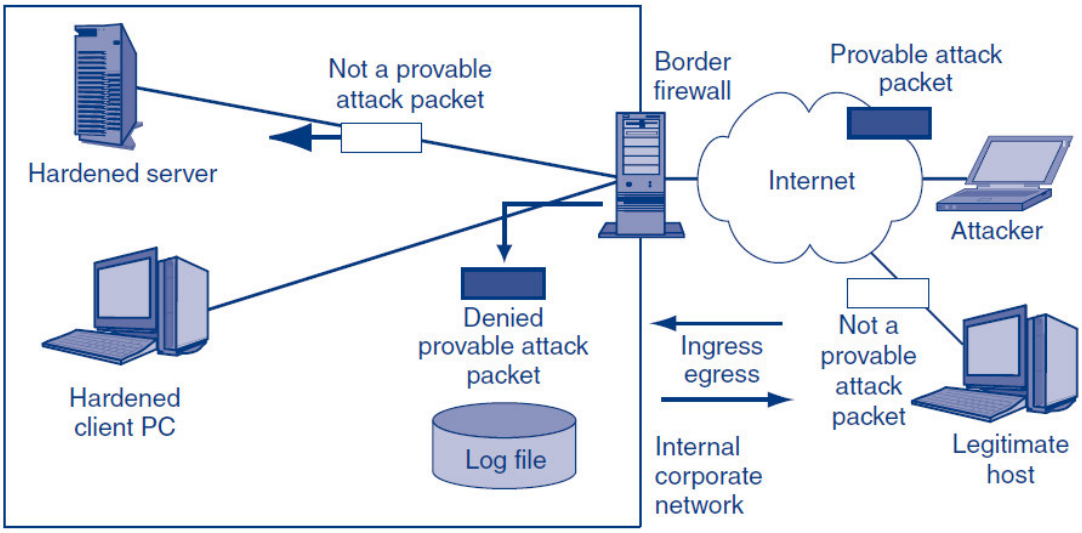


Figura 5. Esquema de funcionamiento de un Firewall en una infraestructura corporativa

Fuente: (Boyle & Panko, 2013, pág. 314)

Stribe (2004, pág. 74) refiere tres funciones fundamentales que cumple casi todo firewall moderno para proveer un servicio de seguridad:

- Filtrado de Paquetes.
- NAT (network address traslation).

- Servicio de Proxy.

En ese mismo contexto, se debe aclarar que el firewall cuenta, en términos muy generales, con distintos mecanismos de filtrado para examinar paquetes que no se los detalla en el presente documento pero sin embargo se los menciona a continuación:

- Stateful packet filtering methods
- Static packet filtering
- Network address translation
- Application proxy filtering
- Intrusión prevention system filtering
- Antivirus filtering

En el ámbito empresarial, mayormente se realiza procesos contractuales con por lo menos dos empresas que brindan servicios de enlaces de datos dedicados para garantizar disponibilidad de acceso a redes externas o hacia redes corporativas propias pero distantes.

Es relevante mencionar que es muy común que en los firewalls principales de perímetro utilizan stateful packet filtering como su mecanismo principal de filtrado e inspección y cualquier otro mecanismo listado anteriormente como filtrado secundario -(…) (Boyle & Panko, 2013). La figura 6 ejemplifica lo citado.

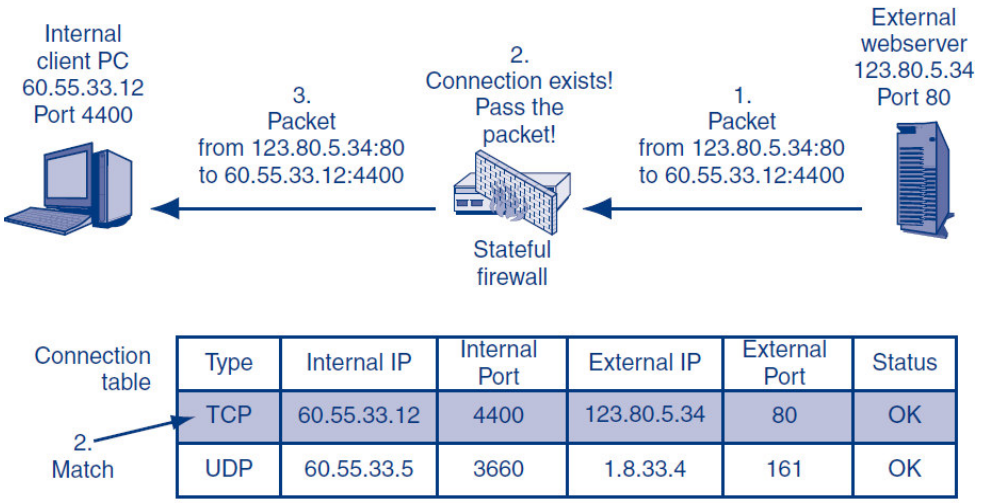


Figura 6. Filtrado por estado de paquetes ó stateful packet filtering.

Fuente: (Boyle & Panko, 2013, pág. 329)

2.2.1.2 Intrusion Detection System

Los sistemas y mecanismos de protección son cada vez más complejos e incluyen algoritmos avanzados para cumplir con su objetivo, sin embargo aquella frase que dice *no hay sistema completamente seguro* da lugar a pensar en que los actuales sistemas de seguridad corporativa contemplan componentes que interconectados funcionan como un solo sistema que centraliza las funciones de seguridad de la red y por ello se hace pertinente considerar esta frase en virtud de la evolución de los métodos de evasión de seguridad o mecanismos de intrusión que han venido desarrollándose.

Este contenido, identifica implícitamente a los elementos más relevantes que pueden intervenir en contra de una red y que determinan la razón de ser de aquellos sistemas diseñados para detectar intrusiones no autorizadas.

Como ya se mencionó anteriormente en el punto 2.1 Defensa en profundidad y Seguridad Perimetral y en el punto 2.2.1.1 Firewalls, existen modelos y mecanismos que definen los aspectos relevantes a considerar para implementar seguridad en el perímetro de la red, sin

embargo es aconsejable en entornos corporativos contemplar el uso de elementos adicionales que se encarguen de funciones específicas para cerrar al máximo la posibilidad de intrusión y como resultado la afectación a infraestructuras críticas.

El termino infraestructura crítica en su contexto más amplio aplica para aquellas instalaciones tecnológicas, servicios públicos, redes o tecnologías de la información en donde su interrupción afecte alguno o varios servicios básicos para la ciudadanía (Sánchez M. , 2011).

Sin duda que para una institución gubernamental, por ejemplo, será una infraestructura crítica su datacenter, su red de core, sus servicios inalámbricos, etc., equipamiento y servicios que ameriten potenciar su seguridad perimetral con la inclusión de elementos o mecanismos adicionales y más complejos que un firewall como un Sistema de Detección de Intrusos o *Intrusion Detection System* o un Sistema de Prevención de Intrusos o *Intrusion Prevention System*.

Los sistemas de detección de intrusos le atañen gran importancia al presente proyecto de tesis por lo que demandará mayor detalle en su investigación científica para sustentar de mejor manera el marco teórico.

Desde el punto de vista cronológico, los primeros sistemas de detección de intrusiones dan lugar en el año 1980 donde James P. Anderson documentó la necesidad de un mecanismo automatizado para revisar los eventos de seguridad que en aquel entonces lo denominaría *Monitor de Referencias*, como resultado de un encargo de las Fuerzas Aéreas de EEUU (González, 2003, pág. 7) .

De acuerdo a Gonzáles, dicho pionero en la seguridad de la información, propuso un sistema que distinguía ataques internos y externos, apoyados en el permiso de acceso de los usuarios. Posteriormente ideó un sistema para distinguir el comportamiento de las

cuentas de usuario, considerando procesos estadísticos de los patrones de uso de dichas cuentas.

Estas bases dieron inicio a modelos más avanzados como por ejemplo; IDES, Automated Audit Analysis, Discovery, Haystack, MIDAS, NADIR, NSM, Wisdom and Sense, entre otros (González, 2003).

Amerita entonces preguntarse cómo podría un administrador de red enterarse que alguien está irrumpiendo en su red?, considerando que con las condiciones mínimas de seguridad bastaría con un Firewall para hacer uso de políticas que permitan autorizar o no el acceso y a su vez registrar los eventos de autenticación exitosos o no llevados a cabo.

Se define a una *intrusión* como "un acto de una persona de intentar apoderarse para irrumpir en, o mal utilizar un sistema, en violación de una política establecida" (Skrobanek, 2011, pág. 117).

En este contexto, se infiere de manera muy ligera que un IDS o *intrusión detection system* podría considerarse como un sistema que, a diferencia de un Firewall, tenga como función detectar comportamientos erráticos al momento de acceder a un sistema informático.

Sin embargo, muchos autores definen a un IDS de manera integral considerando que poseen funciones complementarias a las de un firewall y se constituyen de por sí en herramientas importantes del arsenal hablando en términos de seguridad informática.

Es así que Strebe (2004, pág. 260), define los IDS como "sistemas de software que detectan intrusiones a nuestra red basada en un número de signos reveladores". La figura 7 muestra un esquema de la ubicación de un IDS en la red corporativa.

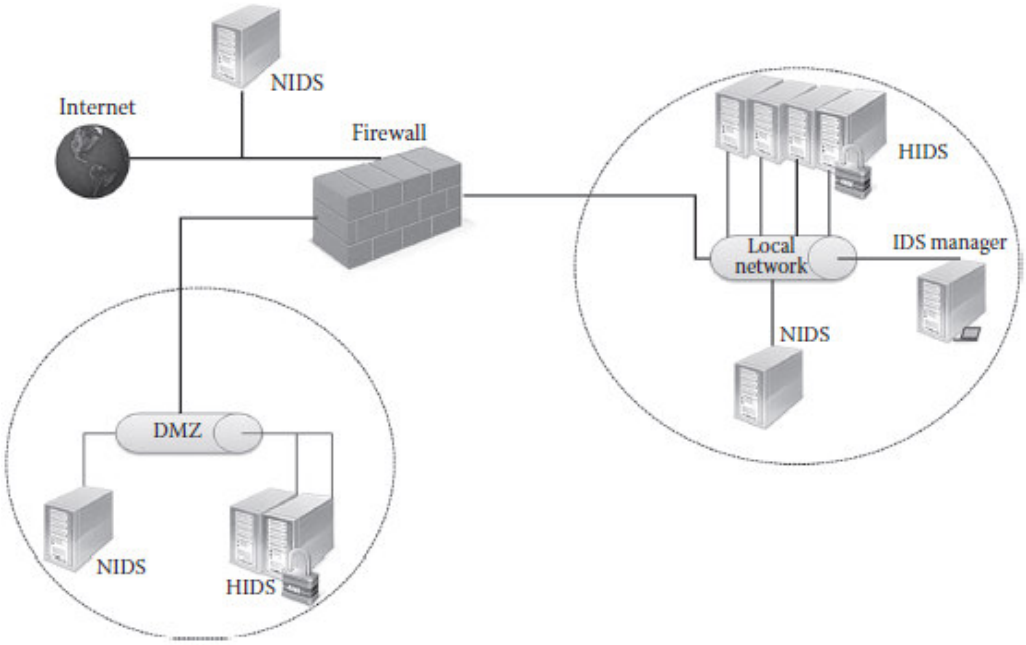


Figura 7. Esquema de localización de un IDS en la red corporativa.

Fuente: (Khan Pathan, 2014, pág. 29)

En esencia, los sistemas de detección de intrusos son una combinación hardware y software que monitorean y analizan cada paquete del tráfico de red con el fin de encontrar patrones de comportamiento anómalo o sospechoso y simplemente alertar a quien administre la red para tomar acciones, lo cual denota que dichos sistemas de seguridad en principio son pasivos, sin embargo también pueden ser activos y detectar y responder ataques (Skrobanek, 2011).

Comercialmente hablando, los IDS tuvieron acogida en el mercado a mediados del año 1997 y a partir de entonces, se han venido creando compañías que han liderado el mercado con soluciones que incluyen *appliances* con funciones integrales de seguridad y han estandarizado la necesidad de contar con estos mecanismos de seguridad a nivel empresarial y gubernamental.

Aunque algunos autores establecen una clasificación bastante amplia de los IDS, para efectos de presente proyecto de tesis se muestran aquellos que son más utilizados y se los son clasifica por la tecnología de detección en la cual están basados; principalmente pueden ser basados en firma y en anomalías como se detalla en la figura 8.

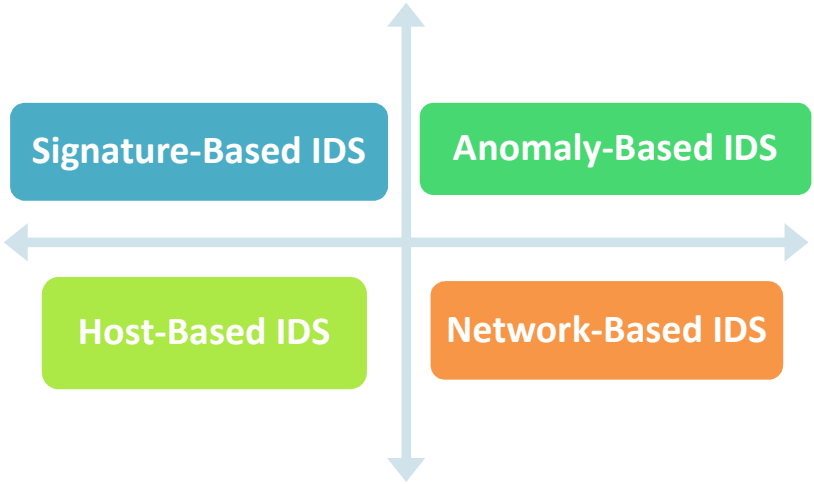


Figura 8. Clasificación de IDS's más utilizados.

En este contexto es pertinente tener claro que un IDS difiere fuertemente de un firewall en su manera de operar, es decir, un firewall se dedica netamente a descartar o eliminar paquetes que pueden ser parte de una intrusión al no cumplir con una política de autorización de acceso, mientras que un IDS detecta paquetes que pueden o no ser una intrusión considerando patrones sospechosos de acceso.

Pathan (2014), menciona algunas de herramientas IDS ampliamente utilizadas hoy en día:

Herramientas IDS basadas en Host:

- OSSEC (Open Source Security)
- Osiris

- Tripwire
- HP_UX HIDS
- CACIC
- Nagios
- Radmind

Herramientas IDS basadas en Red:

- Snort
- ISS
- Kismel
- Cisco Secure IPS
- Prelude IPS
- Bro Intrusion Detection System

2.2.1.3 Intrusion Prevention System

Se considera a la prevención de intrusiones como una técnica proactiva que de alguna manera previene los ataques a la red (Skrobanek, 2011).

En el contexto de un IDS, el sistema de prevención de intrusión o IPS es una combinación de hardware o software que mediante las mismas técnicas de detección y filtrado que utiliza un IDS, puede detener ataques en tiempo real en lugar de únicamente identificarlos y alertarlos.

Es pertinente entonces comentar que a los IDS se los considera como de *primera generación*, teniendo en cuenta las bases documentadas en el año de 1980 mencionadas en el tópico anterior. Sin embargo dentro de la *segunda generación de IDS* se los concibe a los IPS por cuanto tienen características que los podrían considerar como IDS más completos; en conclusión se puede inferir que un IPS es un IDS de segunda generación que según Rhodes (2013), contiene las siguientes características:

- Tipo de IDS y Modelo de Detección.
- Interface de usuario final.
- Administración de IDS.
- Mecanismos de Prevención.
- Desempeño.
- Alarmas y Logs.
- Análisis y Reportes.

La figura 9, muestra de manera práctica la función de un IPS / IDS operando en modo *inline* como punto de inspección filtrando en tiempo real el tráfico que circula de manera bidireccional entre la red interna y la red externa.

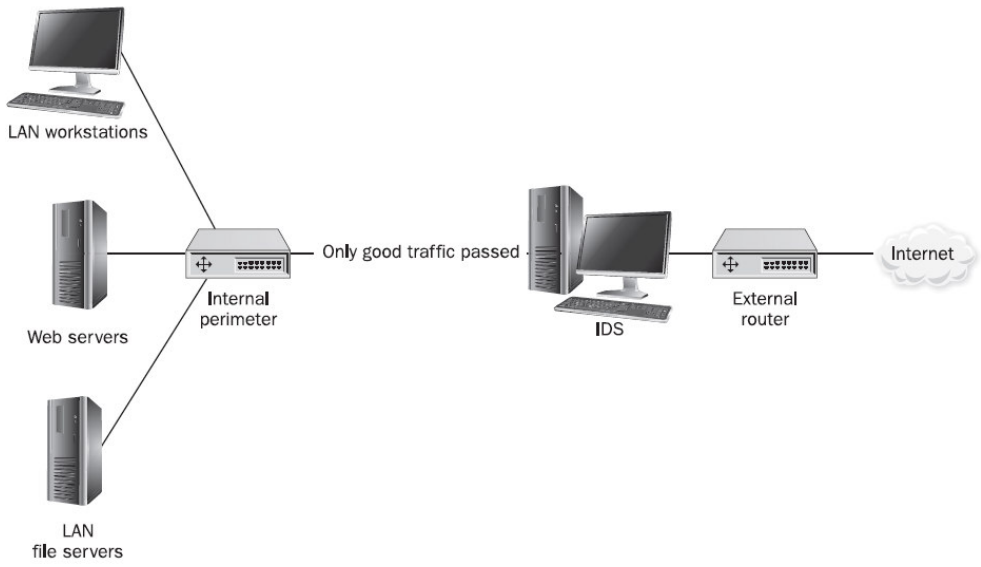


Figura 9: IPS/ IDS en modo in-line ubicado como punto de inspección y filtrado.

Fuente: (Rhodes Ousley, 2013, pág. 414)

Es importante recalcar que para que un IDS pueda realizar un filtrado efectivo y en tiempo real debe analizar el contenido de la carga o "payload" de cada paquete y para ello utiliza hardware basado en tecnología ASIC "circuito integrado para aplicaciones específicas" lo que le provee de mayor velocidad de procesamiento y recursos para tal objetivo.

Como aspecto importante es oportuno mencionar que los IPS principalmente tiene dos acciones específicas al momento de detectar una intrusión: eliminar paquetes y limitar el tráfico de datos basados en el tipo de certeza al momento de detectar dicha intrusión.

2.2.1.3.1 Arquitectura IPS

Aunque la arquitectura de los IDS / IPS varían de un producto a otro, mantienen en común una estructura. En este sentido (Nagenthiran , Jayasekara, & Jayasekara, 2010), refieren

que los componentes de un IDS / IPS son principalmente tres, los cuales dependen de elementos adicionales que se pueden evidenciar en la figura 10.

- **Preprocesador de datos**.- Recolección y formato de datos.
- **Algoritmo de detección**.- Desarrollado en base a un modelo de detección, detecta registros de intrusión normales y malignos.
- **Filtro de alertas.-** Considera la gravedad de la intrusión basado en criterios de decisión y alerta al operador.

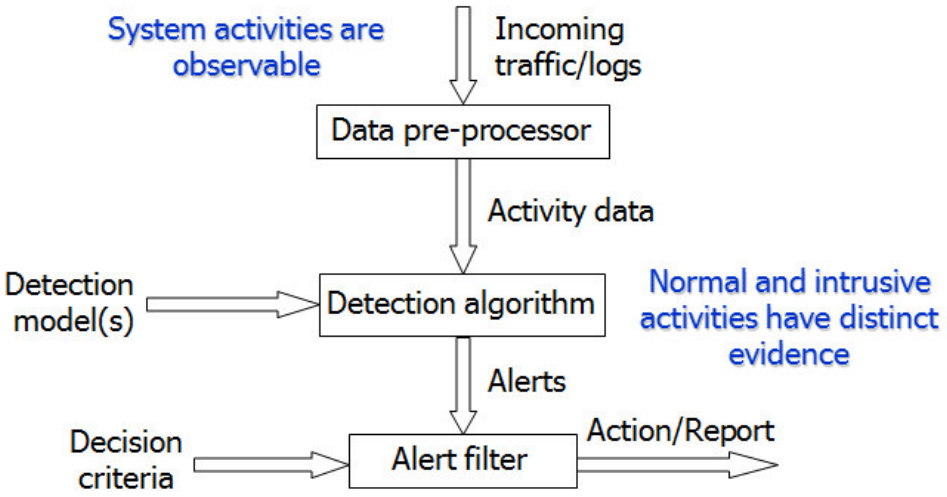


Figura 10: Arquitectura de un IDS / IPS.

Fuente: (Nagenthiran , Jayasekara, & Jayasekara, 2010, pág. 2)

2.2.1.4 IPS según el Cuadrante Mágico de Gartner

El cuadrante mágico de Gartner no es más que una representación gráfica elaborada por la empresa denominada "Grupo Gartner" que principalmente aporta información del mercado sobre nuevas tecnologías en un momento específico.

El ámbito de mercado toma importancia y brinda relevancia al presente proyecto de tesis por cuanto se puede evidenciar las empresas que lideran el mercado a nivel de soluciones tecnológicas y qué características poseen, lo cual a su vez le provee una visión más concreta a quien considere implementar soluciones que cumplan con requisitos planeados.

Es así que (Lawson, Hils, & Neiva, 2015), refieren que el mercado de los appliance IPS está liderado por productos *standlone* o *virtuales* enfocados a realizar su función en la localidad o en la nube. Por otra parte productos como Sistemas de Prevención de Intrusiones de Nueva Generación NGIPS cuentan con funciones avanzadas para prevenir amenazas. En adición a esto, el mercado provee firewalls de nueva generación NGFW con funcionalidades de un IPS y productos *all in one* denominados UTM o *Unified Threat Management* enfocado en pequeñas o medianas empresas.

En la figura 11, se puede apreciar el Cuadrante Mágico de Gartner para los Sistemas de Prevención de Intrusiones más reciente, en donde empresas como CISCO, McAFEE e IBM están definidas como líderes en cumplimiento con diversos criterios de evaluación como por ejemplo: servicios, experiencia, modelo del negocio, innovación, etc.

Figura 11. Cuadrante Mágico de Gartner para IPS a noviembre 2015.

Recuperado de: (Lawson, Hils, & Neiva, 2015, pág. 2)

2.3 Seguridad en Redes 802.11

Según lo refiere (Rhodes Ousley, 2013), las redes inalámbricas conocidas comúnmente como redes wifi estuvieron operando en el año 1969 incluso mucho antes que las redes cableadas basadas en el estándar Ethernet fueran creadas.

No fue sino hasta los años 90´s que se empezaron a utilizar de manera corporativa, con la desventaja de que en aquel entonces fueron propietarias y su mercado era muy pequeño y aunque ha pasado más de dos décadas para que mediante el estándar ANSI/IEEE 802.11 se facilite el desarrollo y la interoperabilidad de este tipo de productos en todo nivel, su evolución ha permitido principalmente mayores prestaciones en temas de movilidad, velocidad, disponibilidad, flexibilidad, bajo costo y sobre todo seguridad, sin embargo los mecanismos para evadir dicha seguridad ha evolucionado paralelamente haciendo de este tipo de redes el objetivo principal para los hackers, obligando a los administradores de red y personal de TI a implementar mecanismos que complementen o reduzcan la posibilidad de intrusiones no autorizadas.

El estándar 802.11 ha permitido generar variantes del mismo para enfocarlos hacia distintas aristas de este tipo de comunicación inalámbrica y aunque en realidad al estándar 802.11 se lo concibe como un grupo o familia de estándares, los más comúnmente utilizados en hogares y empresas son: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g y IEEE 802.11n.

Es por ello que en el ámbito de la seguridad en redes LAN inalámbricas o Wireless LAN se cuentan con mecanismos tan básicos como cifrado de la comunicación mediante protocolos WEP o Wired Equivalent Privacy, WPA y sus variantes, que mediante el uso de una clave para autenticación y encripción intentan reducir la posibilidad de intrusiones

no autorizadas, sin embargo estos mecanismos han sido fácilmente evadidos con herramientas de propósito específico.

Existen otros mecanismos de seguridad inalámbricos más específicos pero no estandarizados que intentan brindar seguridad basados en la dirección física o MAC-address de un equipo final o cliente por ejemplo, en algunos casos son funcionalidades que están incorporadas en los equipos de comunicación, lastimosamente conlleva mucho mantenimiento y generan problemas y en ocasiones son fácilmente vulnerados. (Rhodes Ousley, 2013, pág. 386), refiere a estos mecanismos como: "closed.system SSID, MAC filtering y Protocol Filtering".

- **Closed-system SSID**: Funcionalidad incluida en estaciones base o access points de gama alta, que en términos sencillos consiste en "no difundir el SSID" o el ID de la WLAN. Técnicamente se logra al quitar el campo SSID del "beacon frame" y/o "probe response frames".

- **MAC filtering**: Es una funcionalidad que está actualmente incluida en la mayoría de Access points y que principalmente intenta garantizar conectividad a dispositivos que se encuentren registrados su MAC ADDRESS.

- **Protocol filtering**: Mecanismo de seguridad que está incorporado en todos los Access points actuales y aun que es menos común que los descritos anteriormente, brinda un grado de seguridad al ser selectivo con los protocolos que se utilizaran para conectividad y navegación por ejemplo.

En el presente proyecto de tesis se mencionarán principalmente los mecanismos de seguridad que reducen o mitigan oportunamente los intentos de acceso no autorizado a la infraestructura de la "Empresa Pública de Recaudación de Impuestos".

2.3.1 Arquitectura de las redes 802.11

Según (Chen, Jiahuang, & Zihong, 2013), definen que la arquitectura de una red 802.11 o Wireless LAN está compuesta por *estaciones* que en su conjunto pueden formar un Basic Service Set o BSS y que se comunican mediante el mismo medio inalámbrico común para todas.

Además define que las BSS tiene un identificador que permite reconocerlas, denominado Basic Service Set Identifier o BSSID que no es más que la dirección física del access point que brinda el servicio. En este contexto para identificar individualmente una red WLAN se utiliza un SSID o Service Set Identifier que es un nombre único red de máximo 32 caracteres que será difundido mediante las cabeceras de los frames puestos en el aire como medio de comunicación.

Existen dos categorías de WLAN's consideradas desde el punto de vista de su conexión física o arquitectura de red: infraestructura y ad-hoc.

Una WLAN basada en *infraestructura* se caracteriza por que cada dispositivo cliente dentro de un área de cobertura definida en el estándar IEEE utilizado, establece una conexión inalámbrica con una estación o AP para que solo entonces, puedan intercambiar tráfico en el sentido cliente – AP – cliente. La figura 12 muestra un ejemplo de una WLAN basada en infraestructura.

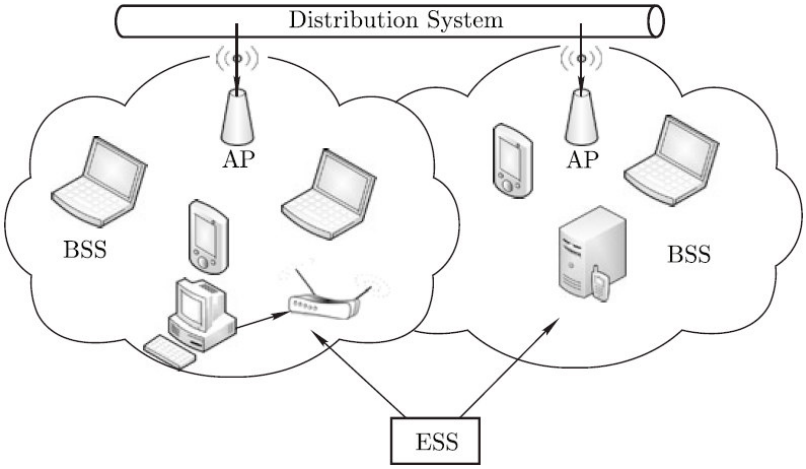


Figura 12. Ejemplo de WLAN basada en infraestructura.

Fuente: (Chen, Jiahuang, & Zihong, 2013, pág. 41).

Una WLAN basada en *ad-hoc* no necesita de una infraestructura o conjunto de estaciones preestablecida ya que en esta categoría cada cliente inalámbrico establece una conexión punto a punto o P2P con cada uno de los otros clientes. La figura 13 muestra un ejemplo de una WLAN basada en *ad-hoc*.

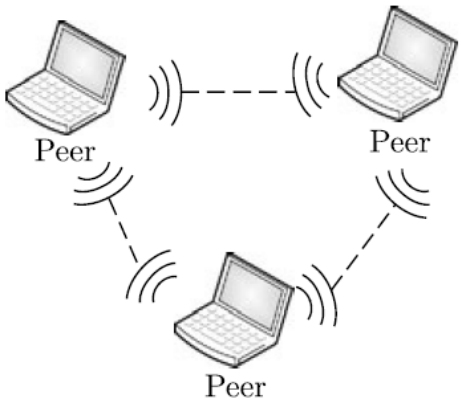


Figura 13. Ejemplo de WLAN basada en ad-hoc.

Fuente: (Chen, Jiahuang, & Zihong, 2013, pág. 41).

2.3.2 Autenticación y Asociación en redes 802.11

Al igual que un PC en una red cableada establece una conexión física con un switch mediante un cable ethernet, igualmente un dispositivo inalámbrico o cliente debe establecer primero un vínculo con la estación para intercambiar datos con la red. Para que un equipo cliente (equipo portátil, Tablet, Smartphone, etc) puede conseguir conectividad con un access point operando en modo infraestructura, el estándar IEEE802.11b definió dos sub procesos que deben realizarse previamente y en un orden específico y solo cuando ello se haya llevado a cabo con éxito, él o los clientes tendrán acceso a la WLAN; dichos sub procesos son:

- Autenticación.
- Asociación.

La autenticación es un proceso que tiene por objetivo verificar la identidad del equipo cliente que intenta conectarse con la estación, es decir confirmar que el cliente es quien dice ser para autorizar la conexión. Dicha autenticación se establece a nivel de capa 2 y puede llevarse a cabo en la misma estación o delegarla a un servicio implementado para tal fin como RADIUS por ejemplo. Según (Coleman & Westcott, 2006), se disponen dos métodos de autenticación:

- Open System Authentication (null authentication).
- Shared Key Authentication.

La asociación en cambio, es un proceso que sucede luego de que el cliente fue autenticado correctamente en la estación, por lo tanto se dice que un cliente se encuentra en estado asociado solo cuando puede intercambiar datos mediante su estación a la cual está conectada y con todos los equipos de su BSS. La figura 14 muestra un ejemplo del proceso de autenticación y asociación en su significado más básico.

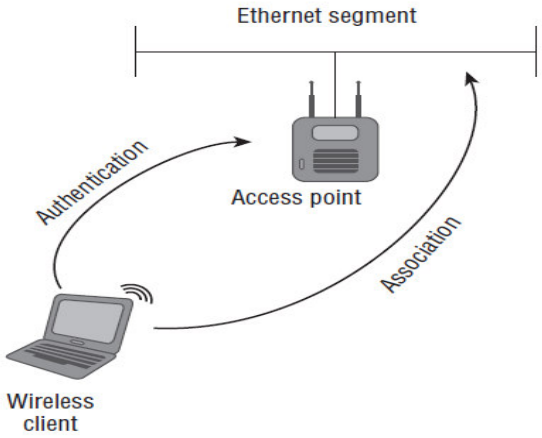


Figura 14: Proceso de autenticación y asociación en un entorno 802.11

Fuente: (Bartz, 2009, pág. 223)

En su conjunto, dichos subprocesos permiten describir la interacción entre una estación y un Access point para lograr una conexión inalámbrica, sin embargo en el transcurso de estos procesos se pueden presentar estados que según define (Holt & Huang, 2010), son tres:

- **No autenticado – No asociado**: Estación cliente completamente desconectada de la red 802.11.
- **Autenticado – No asociado**: Estación cliente autenticada y lista para solicitar asociación con Access point.

- **Autenticado – Asociado**: Estado final en el cual la estación cliente mantiene conexión con un Access point y puede intercambiar tráfico con los componentes de su BSS.

La descripción de estos estados permite comprender de mejor manera esquemas de seguridad en los cuales se vea comprometido algunos de ellos y se intente acceso a la red sin autorización mediante alguna técnica específica.

2.3.3 Mecanismos de seguridad en el estándar 802.11

Los distintos mecanismos de seguridad que se han estandarizado como resultado de la evolución de las redes inalámbricas y sus prestaciones se han constituido como factores indispensables al momento de planificar, diseñar o implementar una red en cualquier escenario y dichos estándares toman mayor importancia en el ámbito empresarial-gubernamental cuando la confidencialidad, integridad y disponibilidad son parte de objetivos estratégicos institucionales.

En el contexto histórico, (Maxim & Pollino, 2002), refieren que la "Local and Metropolitan Area Networks Standards Committee [LMSC]" como parte de la IEEE Institute of Electrical and Electronic Engineers, en el año 1990 forma el grupo de trabajo que definió el primer estándar inalámbrico IEEE conocido como 802.11, bajo el cual se establecían velocidades de 1Mb a 2 Mb usando la banda ISM *industrial, scientific and medical* de 2.4 Ghz.

Este primer estándar definió también los siguientes parámetros:

- Interfaz entre clientes y Access points.

- Capa física y capa MAC.
- WEP como mecanismo de seguridad.
- "Roaming" entre Access points.

La IEEE ha definido una lista muy amplia de estándares y mejoras para la operación de las redes inalámbricas, tanto para las redes que trabajan en la banda de 2.4 Ghz así como para aquellas que trabajan en la banda de 5 Ghz, sin embargo los estándares más comunes así como sus principales características son los que se muestran en la figura 14.

IEEE Standards				
	802.11a	**802.11b**	**802.11g**	**802.11n**
Maximum Throughput	54 Mbps	11 Mbps	54 Mbps	300 Mbps
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz
Modulation	OFDM	DSSS	DSSS/OFDM	OFDM
Channels (FCC/ETSI)	21/19	11/13	11/13	32/32
Ratified	1999	1999	2003	2009

Figura 14: Estándares IEEE 802.11 más comunes.

Fuente: (Stretch, 2016, pág. 1)

2.3.3.1 Wired-Equivalent Privacy – WEP

Según (Tipton & Krause, 2004, pág. 438), "la única técnica que puede asegurar que nadie pueda monitorear fácilmente la transmisión inalámbrica de datos es la encripción".

En este sentido (Earle, 2006, pág. 188) afirma que "WEP es definido como mecanismo criptográfico de confidencialidad opcional usado para proveer confidencialidad de los datos que es subjetivamente equivalente a la confidencialidad de una red de área local alámbrica medio que no emplea técnicas criptográficas para mejorar la privacidad".

En el contexto cronológico de la estandarización de la tecnología 802.11, como se ha mencionado anteriormente, WEP fue uno de los primeros mecanismos de seguridad en ser formalmente aceptado como parte del primer estándar 802.11 con el fin de proveer características de confidencialidad, integridad y autenticación.

Estas características son provistas gracias al algoritmo de cifrado de flujo RC4 que significa Rivest Cipher 4 denominado así por su creador Ron Rivest de la empresa RSA Data Security, Inc. El algoritmo en sí es muy sencillo y reversible porque principalmente es utilizado para la encriptación y desencriptación mediante el uso de sumas de comprobación de redundancia cíclica (Chandra, y otros, 2009). Por otra parte WEP utiliza el algoritmo CRC-32 que significa Cyclic Redundancy Code y una clave secreta compartida pre establecida que en su conjunto le permiten encriptar la comunicación cliente-AP.

Aunque el estándar original 802.11 definió dos versiones de WEP una de 64 bits y otra de 128 bits, se detectaron vulnerabilidades que hicieron de este mecanismo un problema de seguridad.

Según Chen y otros (2013), las principales vulnerabilidades de WEP pueden resumirse en 4 categorías:

- No protección contra falsificaciones.
- No protección contra repeticiones.
- Mal uso de RC4.
- Reutilización de vectores de inicialización.

Los mismos autores mencionan que, WEP es fácilmente vulnerable mediante herramientas como AirSnort, Wepcrack, Wep_tools y haciendo uso de ataques de fuerza bruta, ataques de reutilización de flujos de clave, ataques por debilidad de vector de inicialización.

2.3.3.2 WPA / WPA2

El mecanismo WPA que significa Wi-Fi Protected Access, tiene un contexto histórico de creación bastante particular y es precisamente en donde WEP es vulnerado, que se da inicio a las actividades para mejorar o innovar la seguridad de las redes inalámbricas de su época.

Coleman y otros (2010), refieren que el IEEE 802.11i security task group definió TKIP o Temporal Key Integrity Protocol como una mejora a las vulnerabilidades del protocolo WEP sin necesidad de que el equipamiento deba ser cambiado y simplemente sea necesario un upgrade del firmware. TKIP se enfoca en ampliar la agrupación de IV's vectores de inicialización de 24 bits a 48 bits y usar claves estáticas de 128 bits.

Por otra parte la WI-FI Alliance, siendo una institución que certifica operatividad entre equipos 802.11, unificó esfuerzos y basados en un borrador del estándar 802.11i definió el estándar WPA permitiendo compatibilidad con equipos nuevos de bajos recursos en hardware utilizando RC4 y TKIP.

Entonces, Wi-Fi Protected Access es un protocolo creado para mejorar notablemente la seguridad de las redes inalámbricas enfocándose en solucionar el problema de administración de claves de WEP y el sistema de autenticación de usuarios.

En este sentido Earle (2006), describe que WPA soporta dos métodos de autenticación y administración de claves que se mencionan a continuación:

- Autenticación EAP con estándar 802.1x.
- Soporte WPA para el hogar y pequeñas empresas.

Es oportuno entonces, definir *Extensible Authentication Protocol* EAP, como un estándar de capa 2 concebido originalmente en el RFC 2284 para uso con el protocolo *Point to Point Protocol* PPP y rediseñado posteriormente en RFC 3748 para usarlo con el mecanismo de control de acceso basado en puerto 802.1x.

La característica *extensible* de EAP lo hace capaz de soportar distintas versiones desarrolladas en base éste, pero en esencia su utilidad está en el uso con el estándar IEEE 802.1x para desarrollar procesos de autenticación tanto en redes cableadas así como en redes inalámbricas y principalmente vinculadas a un servidor RADIUS que puede proveer autenticación y administración de usuarios de manera centralizada. Algunos tipos de EAP son:

- EAP-TLS
- TTLS (EAP-MSCHAPv2)
- PEAP (EAP-MSCHAPv2)
- EAP-FAST

En el ámbito de las redes 802.11 corporativas, el protocolo de autenticación *Lightweight Extensible Authentication Protocol* LEAP es propietario de la marca CISCO y principalmente utilizado en sus acccess points pero su codificación está disponible para ciertos fabricantes bajo acuerdo de no divulgación con lo cual amplía su compatibilidad con ciertos clientes inalámbricos.

En contraste a lo mencionado anteriormente, (Oriyano, 2016) refiere a WPA2 como una actualización o un sucesor de WPA que introduce mejoras importantes pero con total compatibilidad con el estándar de seguridad 802.11i.

El mismo autor menciona que WPA2 puede trabajar en dos modos que son:

- **WPA2 Personal**.- Mecanismo de seguridad para uso personal y de SOHO "small office/home office" que permite la autenticación mediante una frase de seguridad.
- **WPA2 Enterprise**.- Mecanismo de seguridad que utiliza 802.1x como método de autenticación basada en puerto y un servidor RADIUS.

En la tabla 1 se muestra un resumen de las características más relevantes para WPA y WPA2.

Tabla 1. Resumen de tipo de seguridad y Mecanismo de cifrado para WPA y WPA2.

Mecanismo de seguridad Wi-Fi Alliance	Mecanismo de Autenticación	Mecanismo de Cifrado
WPA – Personal	Passphrase	TKIP / RC4
WPA - Enterprise	802.1x / EAP	TKIP / RC4
WPA2 – Personal	Passphrase	CCMP / AES or TKIP / RC4
WPA2 - Enterprise	802.1x / EAP	CCMP / AES or TKIP / RC4

Fuente: (Bartz, 2009, pág. 360)

2.3.3.3 Estándar de seguridad IEEE 802.11i

El estándar IEEE 802.11i, que inicialmente estuvo a cargo de *TGe task group* fue reasignado y desarrollado por *TGi security working group* y aunque dicho estándar es técnicamente conocido como 802.11i-2004 por el año de finalización de su desarrollo, es una especificación o enmienda a las vulnerabilidades detectadas en el estándar 802.11

original que al igual que otros estándares intenta garantizar un medio de transmisión inalámbrico seguro.

Earle (2006), describe que algunos de los estándares, protocolos y métodos de cifrado utilizados, fueron creados fuera del estándar y otros dentro del estándar como por ejemplo RADIUS, 802.1x, EAP, AES, RSN, TKIP.

802.11i es un reflejo del mecanismo WPA y WPA2 considerando que sus características son similares, sin embargo, el estándar 802.11i estableció algunos lineamientos previos de lo que sería RSN *robust security network* o Red de Seguridad Robusta, que entre otros, su principal objetivo es esconder u ocultar la información que viaja por el aire.

En este sentido las mejoras incluidas en este estándar son:

- **Privacidad de Datos**.- Mejora la encripción de datos mediante el protocolo CCMP que utiliza AES como mecanismo de encripción.
- **Mejora en Autenticación**.- Se definen dos métodos para autenticación 802.1x o PSK.

La privacidad de datos está delineada por CCMP *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol* que es un protocolo de seguridad propiamente definido dentro del estándar 802.11i que utiliza Advanced Encryption Estándar o AES, un algoritmo de cifrado por bloques que es más seguro que el mecanismo de cifrado de flujo utilizado por RC4, es decir, AES cifra o encripta independientemente cada bloque de 8 a 16 bytes de información y a su vez cambia su orden de manera aleatoria; al final del proceso reinicia su conteo.

El mecanismo *Pre-Shared Key*, permite la autenticación entre un cliente y una estación a través de la utilización de una clave previamente compartida entre dichos componentes.

Según Coleman y otros (2010), la enmienda realizada en el año 2004 para 802.11i ahora forma parte del estándar 802.11-2007 y en ella se define un método de autenticación empresarial y uno para entornos SOHO que en una opinión muy personal coincide en mucho con lo definido por WPA2.

A continuación, la tabla 2 resume las principales opciones de seguridad para las redes 802.11.

Tabla 2. Principales opciones de seguridad para las redes 802.11.

Estándar	Encriptación	Autenticación
Estándar Original IEEE 802.11	WEP	WEP
WPA	TKIP	Passphrase or Radius (802.1x/EAP)
WPA2	AES (TKIP in mixed mode)	Passphrase or Radius (802.1x/EAP)
IEEE 802.11i	AES (TKIP in mixed mode)	Passphrase or Radius (802.1x/EAP)

Fuente: (Graves, 2007, pág. 161)

2.3.3.4 Estándar 802.1x

IEEE 802.1x es el estándar que formalmente define a este mecanismo de control de acceso basado en puerto que aunque inicialmente fue diseñado para trabajar en redes IEEE 802.3 o redes Ethernet, hoy en día es un mecanismo de seguridad que también se lo usa en redes IEEE 802.11 o redes inalámbricas.

El estándar 802.1x provee un esquema de seguridad a nivel de capa 2 permitiendo o denegando conectividad en base a la identidad del usuario, identidad del computador o incluso de ambos. Se dice que es un esquema o mecanismo de seguridad de capa 2 por que si el usuario o equipo es identificado correctamente se asigna una VLAN o una ACL que garantiza su acceso.

Son tres los componentes principales del estándar 802.1x y sus funciones son mencionadas brevemente a continuación:

- **Suplicante**.- Se lo define como el software embebido en el hardware de red de laptops, pcs o dispositivos móviles que desarrolla a nivel de capa 2 y mediante EAP las peticiones de acceso a la red dirigidas al autenticador.

- **Autenticador**.- En términos de redes 802.11 es el Access point o controlador LAN que, ubicado entre el suplicante y el servidor de autenticación, funciona como un mediador para gestionar la comunicación física entre ambos dispositivos para permitir o denegar el acceso. La comunicación entre suplicante y autenticador se efectúa mediante EAP, sin embargo entre el autenticador y el servidor de autenticación es efectuado mediante RADIUS. El autenticador mantiene dos puertos *virtuales* denominados *no controlado* y *controlado*. El puerto virtual *no controlado* permite únicamente el tráfico de autenticación EAP, mientras que el puerto *controlado* bloquea todo tipo de tráfico hasta que la autenticación se efectúe de manera exitosa.

- **Servidor de Autenticación**.- Es el dispositivo que efectúa la autenticación de las credenciales del suplicante y retorna una respuesta o resultado al autenticador autorizando o denegando el acceso dependiendo si la autenticación fue exitosa o no. Es relevante aclarar que el servidor de autenticación puede mantener una base de datos de usuarios o integrarse con bases de datos más extensas y complejas como *Lightweight Directory Access Protocol* LDAP.

2.4 Riesgos y Amenazas frecuentes en redes 802.11

Como ya se ha mencionado anteriormente, la conectividad en redes inalámbricas es una ventaja que solo puede ser aprovechada a través ondas de radio en un medio compartido, no guiado, como es el Aire, sin embargo ello representa un potencial problema de seguridad considerando que incluso los mecanismos para garantizar dicha seguridad como WEP, WPA, WPA2, etc., tienen vulnerabilidades. Por otra parte, estas seguridades se han visto afectadas por mecanismos y herramientas en hardware y software que proveen o facilitan la posibilidad de intentar obtener acceso no autorizado.

Existe la suficiente documentación que respalda y evidencia que los intentos de acceso no autorizado se presentan no solo a nivel de redes inalámbricas sino también en redes cableadas, sin embargo éstas últimas no derivan en el ámbito de análisis del presente proyecto de tesis.

Es muy común que los equipos inalámbricos van mejorando su tecnología dotándoles de características como potencia, seguridad, gestión, etc., sin embargo cuando estos equipos no son utilizados para proveer un servicio de acceso inalámbrico y garantizar la movilidad a usuarios autorizados se incurre en acciones para satisfacer intereses personales que en la actualidad son conocidas como ataques.

2.4.1 Vulnerabilidades de protocolos 802.11

Con el paso del tiempo se han hecho evidentes las debilidades en protocolos que gobiernan la transmisión de datos y su seguridad en redes 802.11. Como se ha mencionado en el punto 2.3.3.1 Wired Equivalent Privacy, son varios los problemas que WEP presenta como mecanismo de seguridad y actualmente no es recomendada su utilización. Se debe destacar que entre sus principales debilidades radica que no soporta reinyección de paquetes, no

dispone de protección contra paquetes falsificados y reutiliza vectores de inicialización lo cual lo hace un protocolo completamente débil incluso contra herramientas como AirSnort, Wepcrack, Weptools que entre otros ejecutan ataques de fuerza bruta, ataques de reutilización de claves y ataques por debilidad de Vector de Inicialización.

De otro lado, protocolos como WPA fueron objeto de mejoras como por ejemplo TKIP como mecanismo de encriptación de paquetes, incremento de la longitud de la clave de 64 a 128 bits para la encriptación de cada paquete con una clave diferente y el vector de inicialización se incrementó de 24 bits a 48 bits, pero a pesar de ello, un ataque por fuerza bruta obtendría la clave de encriptación con algo de tiempo aprovechando el momento cuando se efectúa el proceso de saludo previo al establecimiento de la comunicación en donde se intercambian claves encriptadas, lo cual denota una vulnerabilidad en este protocolo. WPA es susceptible a ataques del tipo Chop Chop e incluso del tipo DoS. En este sentido De Paz (2010), refiere que un mecanismo para evitar posibles ataques a las redes con seguridad WPA, es que se desconectan por 60 segundos cuando detecten dos intentos de ataque en un periodo menor a un minuto.

WPA2 en cambio incorporó el protocolo *Counter Mode with CBC-MAC Protocol* CCMP para garantizar entre otras cosas la autenticación e integridad de los mensajes y, a pesar que utiliza AES como mecanismo de cifrado se han desarrollado algunos ataques como por ejemplo ataques offline, ataques de desautenticación y ataques de fuerza bruta, este último haciendo uso de herramientas como aircrack-ng, aireplay-ng o KisMAC.

Por otra parte, el estándar 802.11i originalmente se enfocó en definir una red que maneje una seguridad fuerte llamada RSN que basada en el modelo suplicante – autenticador - servidor de autenticación del estándar 802.1x propuso garantizar entro otros, aspectos de seguridad, integridad, confidencialidad, etc.

La flexibilidad con la que fue diseñado el estándar 802.11i permite a RSN interactuar con protocolos de seguridad a nivel de capa MAC como TKIP y CCMP; la compatibilidad es otro factor que garantiza a RSN soportar arquitecturas previas como Autenticación abierta, autenticación de clave compartida y WEP.

Como se mencionó en el ítem 2.3.3.3 Estándar de seguridad IEEE 802.11i, dicho estándar utiliza CCMP con AES como mecanismo de encriptación y siendo éste un mecanismo que eleva el nivel de seguridad a un nivel muy fuerte se creería que no es susceptible de ataques de ningún tipo o aquellos intentos de acceso tomarían décadas en conseguirse siempre y cuando se cuente con una capacidad de procesamiento superior a las actuales.

2.4.2 Ataques a redes 802.11

Para Chen y otros (2013), la seguridad de una red WLAN está complementada con políticas que contemplen no solamente esquemas de seguridad para la instalación, administración y uso de la infraestructura, sino también la convergencia de nueva tecnología a futuro entendiendo siempre las vulnerabilidades y posibles ataques que puedan llevarse a cabo sobre la misma.

Las redes inalámbricas operan tanto en capa 1 como en capa 2 del modelo OSI y aunque muchos de los ataques son desarrollados a nivel de capa 2, existen ciertos ataques que se efectúan a nivel de capa 1 que principalmente tienen por objetivo saturar el medio inalámbrico e indisponer el acceso a una red inalámbrica.

Para (Boyle & Panko, 2013), los ataques a redes inalámbricas pueden ser vistos desde tres ámbitos:

- Acceso no autorizado a la red.
- Ataque *Man In The Middle* utilizando *evil twin*.
- Ataque DoS *Denial of Service* inalámbrico.

2.4.2.1 Acceso no autorizado a la red.

La figura 15, muestra un esquema representativo de una infraestructura de red 802.11 corporativa en donde se identifican dos aspectos muy importantes; las estaciones inalámbricas o Access Point son un punto de comunicación crítica entre el medio cableado y el medio inalámbrico y que al verse comprometidas, facilitarían el acceso a recursos corporativos a personas no autorizadas.

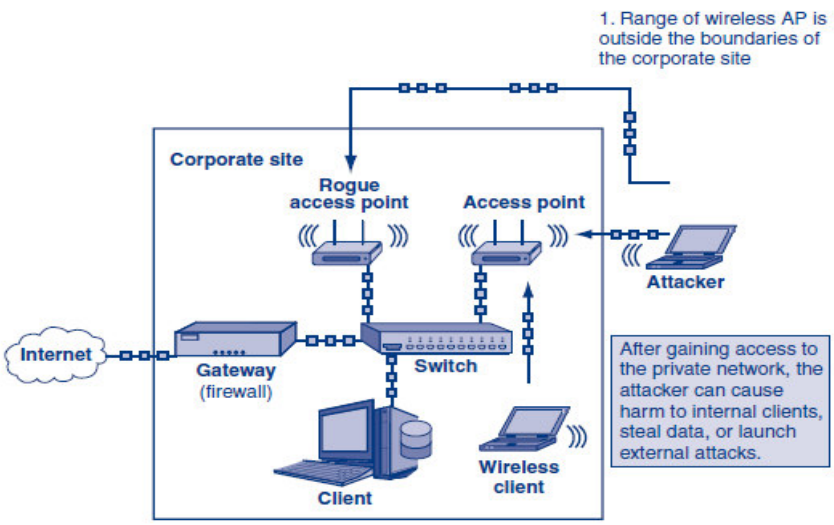


Figura 15: Entorno corporativo 802.11.

Fuente: (Boyle & Panko, 2013, pág. 222)

En este sentido, el acceso no autorizado es uno de las amenazas más comunes a nivel de redes 802.11 en donde los atacantes pueden aprovecharse de las vulnerabilidades de los protocolos de seguridad implementados en los equipos de comunicación.

Por otra parte, la figura 15 expuesta anteriormente, denota que cualquier persona ubicada en las inmediaciones de su objetivo de ataque o incluso alguien que conforma parte del equipo de trabajo de una empresa, puede ubicar un Access point con el afán de conseguir acceso a la red.

Entre los distintos mecanismos para realizar un ataque de acceso no autorizado está el uso de AP's no autorizados o también denominados *Rogue AP* que en su traducción más textual significa *Pícaro*.

- **Rogue Access Point.** Estos dispositivos según Rhodes (2013), son dispositivos que no están autorizados pero que se encuentran conectados a la red física corporativa.

La figura 16, muestra un ejemplo más claro del significado y la función que cumple un Rogue AP al momento de perpetrarse un ataque en donde un Access point conectado a la red física y sin las configuraciones de seguridad apropiadas facilitan a un usuario no autorizado la posibilidad de acceso.

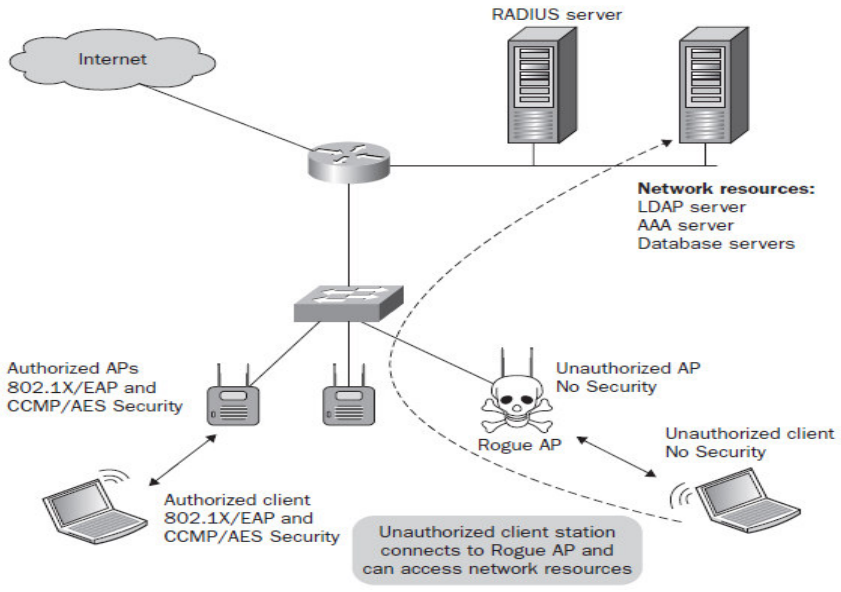


Figura 16. Ataque mediante Rogue AP en entorno inalámbrico corporativo.

Fuente: (Coleman, Westcott, Harkins, & Jackman, 2010, pág. 293)

Según Chen y otros (2013), los ataques mediante Rogue AP así como aquellos que hacen uso de técnicas como MAC Spoofing e IP Spoofing son catalogados como ataques de desautenticación en donde su objetivo es robar la identidad de los usuarios legítimos.

Los mecanismos de MAC Spoofing e IP Spoofing tienen en común la característica de alterar la dirección física o la dirección IP de las tarjetas de red inalámbricas para aparentar ser clientes legítimos con el fin de evadir políticas de control de acceso basadas en dichos parámetros y con ello ganar acceso a la red.

2.4.2.2 Ataque "Man in the Middle"

Este ataque es también conocido como MITM y consiste principalmente en utilizar un computador conocido como *evil twin* o *gemelo malvado* que cuenta con el hardware y software adecuado para simular un Access point que difunde un SSID idéntico al corporativo y preferentemente de mayor potencia, con el afán de aparentar legitimidad y conseguir clientes que al conectarse puedan generar tráfico que puede ser leído por el atacante.

La figura 17 muestra de manera gráfica el funcionamiento de este tipo de ataques.

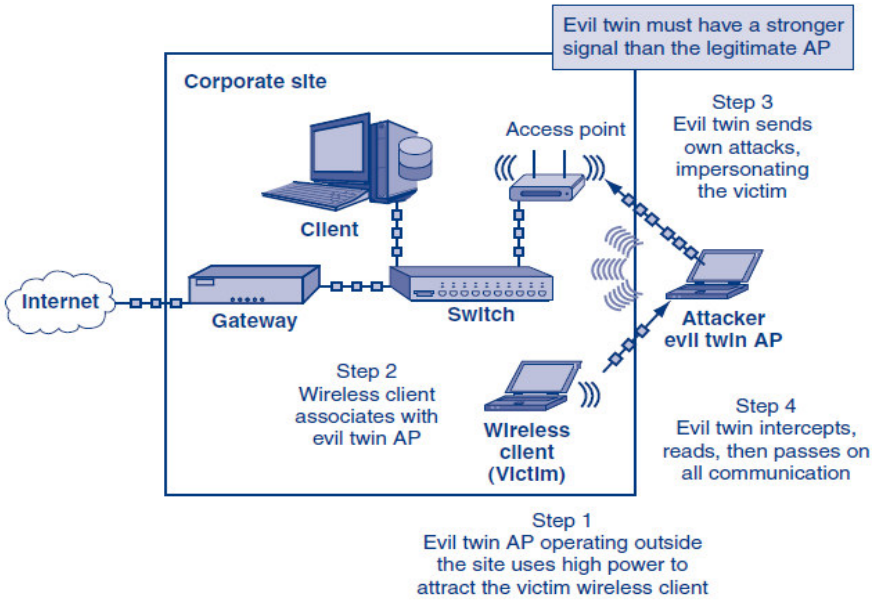


Figura 17. Ataque MITM utilizando evil twin AP.

Fuente: (Boyle & Panko, 2013, pág. 224)

Otros autores clasifican a este tipo de ataque como Ataque de Espionaje o *Eavesdrooping* que suelen ser el primer paso para lanzar otros ataques. Este tipo de ataques consiste en utilizar mecanismos para olfatear y capturar tráfico inalámbrico y conseguir información crítica que les permitan autenticarse en una red 802.11. Para tal objetivo se utilizan herramientas como kismet, Airtraf, Airfart y que muchas de ellas se encuentran dentro de la suite Kali Linux. Dentro de este tipo de ataques se encuentran también Traffic Eavesdrooping, network injection.

2.4.2.3 Denial of Service - DoS

Mejor conocido como *Denegación de Servicio* es un ataque que no solo afecta a redes cableadas sino también a redes 802.11 y consiste básicamente en generar una indisponibilidad de la red a través de impedir que el tráfico legítimo alcance su destino final. Este objetivo es alcanzado al saturar o inundar el medio inalámbrico de señales con

frecuencias mucho más altas, consumiendo su ancho de banda total hasta que ningún componente en la WLAN pueda conectarse.

Otra documentación investigada, cataloga este tipo de ataques como *Traffic Jamming* que significa *Interferencia de tráfico* y que principalmente aprovecha la vulnerabilidad que se presenta en redes 802.11 a nivel de su capa física.

Boyle y Panko (2013), resaltan tres tipos de ataques que pueden generar Denegación de Servicio y que se resumen a continuación en la tabla 3.

Tabla 3. Tipos de ataques DoS.

TIPO DE ATAQUE DoS	METODO	FUENTE	DETECCIÓN
FLOOD THE FRECUENCY	Interferencia electromagnética	Teléfono inalámbrico, horno microondas, dispositivo bluetooth, etc.	Analizador de espectro.
FLOOD THE ACCES POINT	sobrecarga de AP	Envío desordenado de paquetes al AP o envío constante de archivos pesados.	n/d
SEND ATTACK COMMANDS	inyección de paquetes/ mensajes de desautenticación	envío de frames de control o administración / frames RTS - CTS	n/d

Fuente: Adaptado de (Boyle & Panko, 2013).

Otros tipos de ataques que deben ser considerados son aquellos que se enfocan en vulnerabilidades implícitas en el estándar 802.11 y en sus protocolos de seguridad implementados o incluso en la configuración de los equipos que brindan conectividad inalámbrica.

- **Ataques de fuerza bruta y configuración errónea**.- Aunque este tipo de ataques pretenden abusar de la inexperiencia o desconocimiento de quienes administran una infraestructura informática, existen métodos para forzar la obtención de una clave de acceso a un Access point por ejemplo, permitiéndole a un atacante comprometer

incluso la WLAN entera. Para realizar este tipo de ataque se utiliza software de propósito específico como Kali Linux el cual incluye gran cantidad de herramientas que permiten aprovechar por ejemplo las vulnerabilidades de los mecanismos WEP, WPA, WPA2.

2.5 Wireless Intrusion Prevention System (WIPS)

En el contexto de la seguridad de una infraestructura inalámbrica, en el presente proyecto de tesis se ha dicho lo suficiente para argumentar las vulnerabilidades que éste tipo de infraestructuras debe manejar con el afán de reducir el impacto si es que un ataque ocurriese. Como medida complementaria a todos los mecanismos y protocolos que el estándar 802.11 dispone en la actualidad, las marcas más reconocidas a nivel mundial líderes en soluciones de conectividad han implementado tecnologías para detectar e incluso prevenir ataques de índole malicioso desarrollando soluciones en hardware y software que permiten integrar las funcionalidades de un IPS en el ámbito de las redes 802.11.

Según la definición de un IPS desarrollada en el punto 2.2.1.3 Intrusion Prevention Systems del presente proyecto de tesis, un IPS se constituye en una herramienta que refuerza las políticas de seguridad previniendo la ejecución de un ataque mediante mecanismos de identificación, notificación e incluso contención.

Desde un punto de vista de buenas prácticas para el aseguramiento de infraestructuras basadas en el estándar 802.11, el monitoreo es un proceso fundamental para perfeccionar la seguridad de la misma y para ello tecnologías como WIDS /WIPS proveen capacidades para un monitoreo constante.

De acuerdo a Ciampa (2013), son varias las desventajas de los sistemas inalámbricos de detección de intrusiones WIDS, sin embargo resalta que a diferencia de éste, un sistema

inalámbrico de prevención de intrusiones WIPS es una herramienta proactiva de monitoreo que sondea el tráfico de red 802.11 y actúa de manera inmediata bloqueando un ataque malicioso.

Considerando este criterio, es muy relevante contrastarlo con la definición formal que Bartz (2009, pág. 223), refiere indicando que un WIPS es una solución hardware / software que monitorea las ondas de radiofrecuencia mediante un sensor inalámbrico (hardware) y toma las acciones apropiadas en función de comparar el comportamiento de acceso de una estación cliente con una BDD de firmas de intrusión.

Son muchas las ventajas que los sistemas WIPS proveen a un ambiente corporativo, entre ellas se pueden mencionar las más relevantes a continuación:

- Monitoreo 24/7.
- Detección de variedad de ataques.
- Reportes completos y detallados.
- Análisis de información forense de información almacenada.
- Administración de políticas de seguridad WIPS.

2.5.1 Arquitectura de WIPS.

Como se ha mencionado anteriormente, un IPS es un IDS con funciones mejoradas, de ahí que análogamente la arquitectura de un WIPS está constituida de elementos hardware y funciones similares a los de un WIDS.

Una solución WIPS en su concepción más básica está fundamentada en un modelo cliente – servidor que consta de tres componentes principales que son: Servidor WIPS, Consola

de administración y sensores. Estos componentes pueden observarse de manera muy práctica y sencilla a continuación en la figura 18.

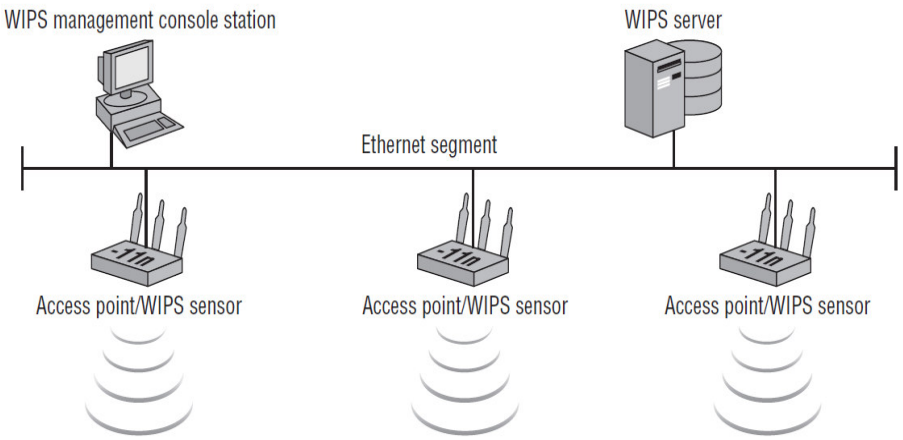


Figura 18. Arquitectura solución basada en Wireless Intrussion Prevention System

Fuente: (Bartz, 2009, pág. 341)

2.5.1.1 Servidor WIPS.

Este componente se define como el punto central de administración y gestión de la tecnología WIPS. Típicamente se presentan como soluciones propietarias hardware en appliances dedicados con características enfocadas a brindar altas prestaciones y por otra parte pueden ser implementados como soluciones software virtualizadas anidadas en la infraestructura de red empresarial.

El servidor WIPS es el principal componente de una solución de prevención de intrusiones inalámbricas ya que éste contiene la lógica para desarrollar el análisis de anomalías, patrones sospechosos, detección de frames modificados, monitoreo radio frecuencia y ruido en el entorno inalámbrico.

Como elemento indispensable y que no se lo menciona en algunas fuentes bibliográficas está la BDD que dependiendo de la infraestructura puede está implementada como parte del servidor WIPS o como un servidor dedicado. En ciertas soluciones de la marca CISCO por ejemplo incluyen una BDD en el mismo servidor WIPS en donde se almacena eventos, registros, logs e incluso la BDD de firmas.

2.5.1.2 Consola de administración WIPS.

La consola de administración o gestión de una solución WIPS está basada en software y no es más que la interface gráfica que generalmente es un browser mediante el cual usuarios y administradores de red pueden interactuar con el servidor WIPS desde cualquier terminal autorizado conectado a la red.

2.5.1.3 Sensor inalámbrico WIPS.

Un sensor inalámbrico en el ámbito de las redes inalámbricas 802.11 no es más que un hardware o software dedicado al monitoreo y recolección de información relevante para que posteriormente sea analizada por el servidor WIPS.

En la mayoría de soluciones de seguridad inalámbrica los sensores inalámbricos hacen uso de los chipsets de radio 802.11 o incluso el mismo hardware de los AP's para monitorear el medio. Ciampa (2013), menciona que a estos sensores también se los denomina *sensores AP* o incluso *sensores embebidos*. La principal desventaja de este tipo de sensores es que por una parte el AP que monitorea el medio inalámbrico no puede brindar el servicio de conectividad es decir no difunde ninguna SSID, por otra parte de acuerdo a lo referido por Timofte (2008, pág. 129), este tipo de sensores no puede monitorear el tráfico de todos los

canales de una banda, únicamente monitorea un canal a la vez y mediante la técnica *channel scanning* monitorea cada canal de la banda en uso, algunas veces por segundo.

Por otra parte los fabricantes han desarrollado los denominados sensores inalámbricos sobrepuestos que no son más que módulos dedicados que se acoplan a los AP que están implementados en una infraestructura inalámbrica para que de esta manera el monitoreo no impacte en el desempeño de la red inalámbrica. Cisco por ejemplo cuenta con el módulo WSM AIR-RM3000M para AP's de la línea Aironet, el cual provee monitoreo dedicado sin afectar el performance del AP sobre el cual está montado (CISCO). La figura 19 muestra un ejemplo de módulo WSM mencionado.

Figura 19. Ejemplo Modulo CISCO WSM AIR-RM3000M

Fuente: (CISCO)

2.5.2 Detección y prevención de Intrusos

Una de las razones por las cuales un WIPS es una herramienta que previene intrusiones es porque cuenta con la capacidad de mitigar o contener accesos no autorizados por medios ilegales desde dispositivos etiquetados como *ROGUES* sean AP o clientes.

Textualmente la palabra *Rogue* tiene un significado que denota pircadía, inconformidad, deshonestidad, ocultación y en informática es un término acuñado a todo dispositivo

estación o cliente inalámbrico que puede o no estar conectado a la red cableada de una empresa sin contar con la autorización de quien administra dicha red y que sus propósitos sean maliciosos. A este tipo de dispositivos también se los denomina *Evil Twin* y su definición textual de *Gemelo Malvado* manifiesta su función.

En este sentido una de las funciones principales de los sistemas de prevención de intrusiones inalámbricas es clasificación de dispositivos y para ello la mayoría cuenta con cuatro categorías como se menciona a continuación:

- **Dispositivo de la Infraestructura**.- Cliente o AP autorizado.
- **Dispositivo desconocido**.- Cliente o AP detectado pero no autorizado.
- **Dispositivo Conocido**.- Cliente o AP de identidad conocida. Dispositivos cercanos.
- **Dispositivo Fantasma (Rogue).-** Cliente o AP que representan amenaza potencial por estar conectado al core de la infraestructura o en algún punto de la red inalámbrica y no estar administrado por la empresa.

Según refiere Timofte (2008), los sistemas de prevención de intrusiones pueden detectar eventos usando tres metodologías: detección basada en firmas, detección basada en anomalías y detección basada en análisis de estado del protocolo. Se puede ver una explicación de cada uno a continuación en la figura 20.

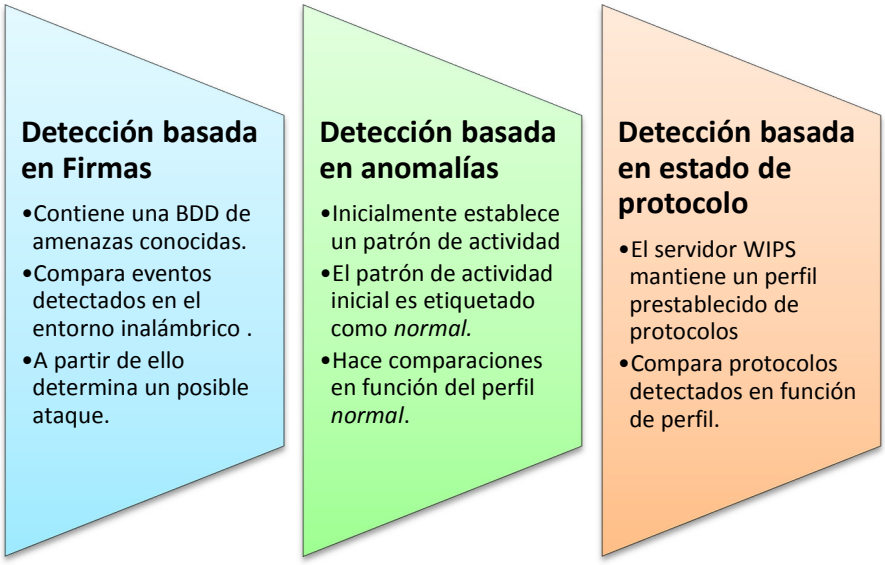


Figura 20. Metodologías de detección de Intrusiones.

Fuente: Adaptado de (Timofte, 2008)

2.5.3 Monitoreo y Alertas.

El método de visualización de eventos e incidentes en una red inalámbrica es el monitoreo y como tal es llevado a cabo únicamente a través de los AP's desplegados a lo largo de toda la infraestructura inalámbrica; de manera análoga, dichos AP's son los ojos y oídos del administrador de red.

Es así que dicho monitoreo utiliza los dispositivos de radiofrecuencia o radios para realizar un escaneo o escucha de manera pasiva para posteriormente transmitir los parámetros relevantes de las conexiones 802.11 hacia el servidor WIPS enfocándose principalmente en incidentes a nivel de capa 2 e incluso a nivel de capa 3 si el dispositivo no autorizado está con una configuración válida.

Dicho monitoreo se efectúa principalmente en los 14 canales de la banda 2.4Ghz ISM así como en todos los canales de la banda 5Gh U-NII.

De acuerdo a Sánchez y Martínez (2008), las posibles amenazas inalámbricas que un WIDS / WIPS puede detectar son las resumidas a continuación en la tabla 4.

Tabla 4. Posibles amenazas inalámbricas detectables por IDS/IPS.

Attack Type	Attack Name
Passive	War Driving
	Man-in-the-Middle Attack
	High-Power Amplifiers
	Dictionary Attack–WPA
Masquerade	MAC Address Spoofing
	Bypassing Access Control List
	Authenticated User Impersonation
	Invalid State
	De-Authentication
	Disassociation
	ARP Poisoning
	MAC-Based Inference of ACL
	Virtual Carrier Sense Attack
Replay	Packet Re-Routing
Modify	Packet alteration
	Packet insertion
Denial of Service	Denial of Service
	RTS/CTS Flood
	Fragmentation Attacks
	Wormhole Attacks
	Network Injection Attacks
	Multiple Virtual Access point

Fuente: (Sánchez & Martínez, 2008, pág. 1799)

Este proceso tendrá resultados óptimos considerando que se desarrolla sobre una arquitectura WIPS distribuida, muy común en ambientes corporativos y gubernamentales en donde cada sensor reporta la información hacia el servidor WIPS en función de las políticas incluidas en su controladora y actúa proactivamente si la política configurada indica alguna acción.

Las alarmas por consiguiente serán factor fundamental para que posibles taques sean reportados y notificados adecuadamente, sin embargo dichas alarmas o alertas, se ejecutarán en función de una correcta configuración de las políticas que disparen eventos verídicos y con ello se evite la notificación de *falsos positivos* que normalmente son comunes en los sistemas de detección de intrusiones.

Las marcas propietarias de los sistemas WIPS implementan una cantidad de alarmas que bordean los 100 posibles riesgos potenciales y por ello Coleman y Westcott (2006), resaltan que una parte importante de un despliegue WIPS es la configuración de sus políticas y sus alarmas contemplando parámetros como severidad y límites de notificación de un ataque.

2.6 Bring Your Own Device

El acceso a la tecnología y su adopción hasta hace unas décadas, tenía una tendencia unidireccional, la cual estaba definida inicialmente por esquemas comerciales y tecnológicos en donde las grandes empresas eran quienes lideraban el consumo de tecnología la cual posteriormente se trasladaba al consumo del usuario, sin embargo esta tendencia ha cambiado tanto que hoy en día la más avanzada tecnología se encuentra empoderada en los usuarios, empleados, personas que cuentan con los equipos de última tecnología en lo referente a movilidad, procesamiento, Internet de las cosas, almacenamiento en la nube e incluso servicios de telepresencia y con ello se ha visto un notorio crecimiento de la demanda por acceso a internet lo que ha revolucionado los entornos empresariales actuales a nivel de América, Asia e incluso países de Europa y Medio Oriente.

Este cambio de direccionalidad de la adopción de tecnología ha definido una tendencia denominada *consumerización* que, a pesar de no estar formalmente definido por la Real Academia de la Lengua Española, es un término también definido como *consumerización de TI* y acuñado a la tendencia de consumo que ocurre primeramente en el entorno de los empleados y posteriormente se traslada hacia el ámbito gubernamental y comercial.

Complementario a lo mencionado en el párrafo anterior, Microsoft (2011) define que la consumerización es "…la tendencia creciente según la cual los usuarios corporativos terminan por decidir qué dispositivos, aplicaciones y servicios se usan en el empleo".

Así, la figura 21, confirma esta tendencia en función de un estudio realizado por la empresa International Data Corporation en donde el porcentaje de conectividad de dispositivos móviles proyectada para el año 2017 estará liderado tanto por smatphone's como por tablet's.

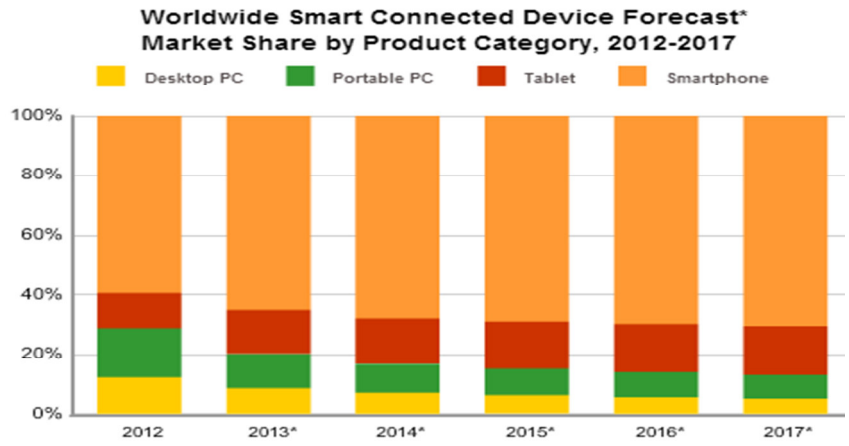


Figura 21. Proyección de conectividad de dispositivos móviles para el 2017.

Fuente: (Columbus Luis, 2013)

Las estadísticas, proyecciones y preferencias empresariales que la consumerización ha traído consigo se ha sumado a la creciente demanda de servicios de acceso a internet que

la tecnología celular 4G ha satisfecho promoviendo varias tendencias empresariales en donde el empleado ha ido imponiendo en su lugar de trabajo con la premisa de mejorar la productividad.

Dichas tendencias se han formalizado con esquemas como *Bring Your Own Device* o mejor conocida como *BYOD*.

BYOD son las iniciales de la tendencia empresarial *Trae tu Propio Dispositivo* en la cual se concibe el concepto de que el empleado traiga su propio equipo móvil, tablet o Smartphone, con el cual pueda acceder a recursos corporativos y realizar tareas laborales que habitualmente realiza con la infraestructura tradicional que la empresa provee. Los principales recursos corporativos a los que se accede son: e-mails, bdd, archivos en servidores, aplicaciones del negocio, entre otros.

Este concepto se ha estado adoptado en otros entornos como en el educativo, en el ámbito médico, etc, en donde según refiere Melero (2014), se han concebido variantes de dicha tendencia, que aunque no son motivo del presente proyecto de tesis se las menciona a continuación:

- BYOC Bring your own Computer.
- BYOA Bring your own App.
- BYOL Bring your own Laptop.
- BYON Bring your own Network.
- BYOT Bring your own Tecnology.

Según algunos autores, Melero (2014) y Alonzo (2013), refieren que BYOD tiene un posible origen en la alta gerencia, cuando en el año 2007 apareció el iphone de Apple que

cambió la perspectiva de quienes gustaban de los dispositivos BlackBerry y que encontraron una herramienta ligera y apropiada incluso para llevar consigo al trabajo.

Otra tendencia que se ha hecho presente es la denominada CYOD abreviada así por su significado de *Escoja su propio Dispositivo* o *Choose your own Device*, la cual contempla el aprovisionamiento de dispositivos móviles de parte de la empresa hacia los empleados que sin duda tiene el aspecto económico en contra de la iniciativa BYOD.

2.6.1 Ventajas y Desventajas

Adoptar la tendencia BYOD supone cambios, ventajas y nuevos retos para quienes administran una red empresarial y esto en general tiene un impacto para la empresa por cuanto también conlleva desventajas que deben ser consideradas.

Entre sus principales ventajas se puede destacar aquellas que son significativas para la empresa así como para el empleado. Es así que adoptar un esquema BYOD es muy ventajoso por que incrementa la productividad de los empleados al tener la comodidad de trabajar con un solo dispositivo, reducción de costos para la empresa al no incluir en sus gastos el costo de hardware, licenciamiento, comunicaciones, portabilidad, rapidez, gestión, ubiquidad etc.,

De otro lado, existen algunas desventajas, riesgos y amenazas que deben ser tomadas en cuenta como por ejemplo la seguridad de los dispositivos, el robo de información crítica, riesgo de malware y otros tipos de software malicioso, compatibilidad, soporte técnico, necesidad de un sistema de administración de movilidad, entre otras que incluso se hacen más evidentes en el escenario supuesto de una pérdida del dispositivo móvil.

Existen esquemas de implementación de BYOD en donde la empresa subsidia cierto porcentaje al empleado por concepto de uso y mantenimiento enfocados en smatphones,

sin embargo para el caso de tablet's u otro tipo de dispositivo móvil es muy ocacional y depende de la liquidez de la empresa.

Para que el esquema BYOD pueda tener éxito, es importante delimitar la responsabilidad de la empresa y la que corresponde al empleado en el buen manejo de la información, es decir, al ser un dispositivo de propiedad del empleado la empresa no puede garantizar un control total en escenarios en los cuales el dispositivo se pierda o sea robado e incluso en el caso en el cual el mismo funcionario mal utilice dicha información utilizando el dispositivo para otros propósitos. En este escenario se debe tener en cuenta que el dispositivo que utilice el empleado contendrá información tanto personal como corporativa. Este aspecto denota la necesidad de esquemas de control y monitoreo como MDM para garantizar una supervisión más estricta de la información que se almacena en un smatphone y los contingentes a realizar en caso de pérdida o robo.

A continuación, la figura 22, muestra la interacción que tendría un esquema BYOD orientado a una infraestructura inalámbrica institucional en donde se evidencia que la autorización asigna un rol y mediante distintos SSID se provee una segmentación para discriminar el nivel de acceso de cada usuario.

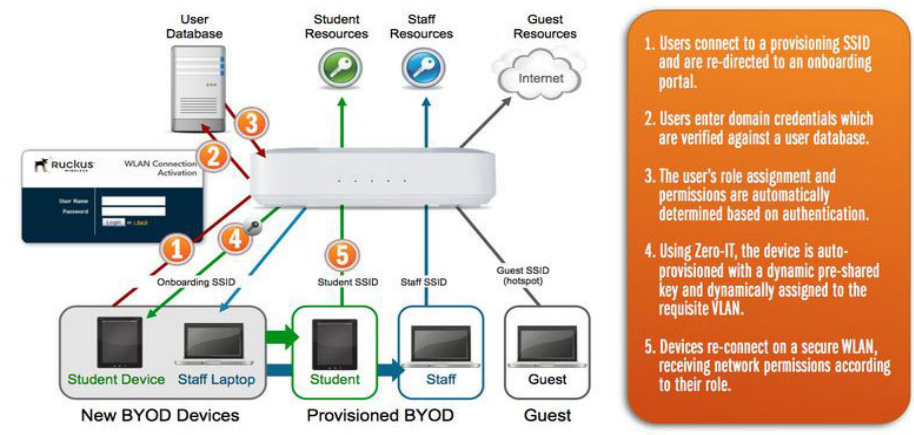


Figura 22. Esquema BYOD ejemplo para infraestructura inalámbrica.

Fuente: (RUCKUS, 2016)

En América Latina son muchos los casos de éxito al adoptar un esquema BYOD, ejemplo de ello es la iniciativa adoptada por la Academia Cotopaxi (s.f.) en Quito-Ecuador, quienes han implementado un esquema BYOD en el cual durante dos años a partir del periodo lectivo 2016-2017 y 2017-2018 los estudiantes comprendidos entre los 3ros y 12vos grados traen su propio dispositivo a su lugar de estudios para potenciar el aprendizaje en la comodidad de sus dispositivos y haciendo uso de herramientas colaborativas que le brinda la posibilidad de iniciar tareas en su centro de estudios y posteriormente continuarlos en sus hogares como una de sus principales ventajas.

Ahora bien, no cabe duda que a la fecha de elaboración del presente proyecto de tesis, existen estadísticas, documentos, artículos e incluso trabajos académicos que pretenden dar una perspectiva muy negativa acerca de la adopción de un esquema BYOD, sin embargo es evidente que la realidad en empresas públicas y privadas en Ecuador indique un escenario en el cual el empleado promedio analista, especialista o experto requiera interactuar con información, correos, aplicaciones y demás data corporativa en momentos críticos, para lo cual es importante contar con un acercamiento que permita a futuro delimitar bajo qué condiciones pueden permitirse dichas interacciones sin poner en riesgo o comprometer la información institucional.

2.6.2 Mobile Device Management

Es evidente que al adoptar un esquema empresarial BYOD existen riesgos y desventajas que deben ser evaluados desde puntos de vista económicos, técnicos y jurídicos, pero existen mecanismos para contrarrestar aquellos riesgos implícitos en la utilización de dispositivos de propiedad del empleado como por ejemplo los sistemas de gestión de dispositivos móviles o Mobile Device Management.

Según refiere (Giusto Bilić, 2016) son dos los enfoques que MDM presenta; Mobile Application Management MAM y Mobile Information Management MIM, el primero es encargado de controlar el acceso a ciertos aplicativos a determinados usuarios e incluso desde ciertos dispositivos mientras que el segundo enfoque garantiza que la comunicación de la información institucional sea realizada desde y hacia dispositivos autenticados.

Para definir la funcionalidad de un sistema MDM es importante realizar un acercamiento a los componentes de un esquema de administración de movilidad empresarial EMM como paso previo a desarrollar una política para un esquema BYOD.

Dichos componentes según (Diogenes & Gilbert, 2015) son referidos como: Usuario, Dispositivo, Data y Apps.

Para un esquema MDM los usuarios que eligen su propio dispositivo para utilizar recursos del trabajo utilizaran el mismo para tareas personales y a su vez los directivos de la empresa desean mantener el control de dichos dispositivos.

Por otra parte el dispositivo y las aplicaciones deben estar con un cierto nivel de control que permita a la empresa contar con la capacidad de gestionar actualizaciones, accesos controlados por credenciales, compatibilidad de las aplicaciones para distintos dispositivos y capacidad de gestión de dispositivos propios y ajenos a la empresa.

La data, por otra parte, es un activo intangible de la empresa pero tan o más valorado que los mismos dispositivos informáticos y por ello debe permanecer en el data center institucional manteniendo un esquema de acceso vía web para aquellos equipos ajenos a la institución.

En donde BYOD tiene falencias, es donde un esquema MDM opera, complementando aquellas posibles inexactitudes que pueda tener cada componente como por ejemplo: seguridad, control, visibilidad por parte de TI e incluso adopción por parte de usuario.

Es así que para citar algunos ejemplos de esquemas MDM está Intune de Microsoft, Air-Watch de VM Ware, MaaS360 de IBM, entre otros.

2.6.3 Políticas BYOD.

Una política de seguridad en el ámbito de la informática es "…un conjunto de reglas para mantenimiento de cierto nivel de seguridad" (Wikipedia, 2015).

De manera complementaria, (Wikipedia, 2015), concibe a una política de seguridad como un documento de alto nivel que puede ser único o inserto en algún otro documento afín que contiene lineamientos para garantizar la seguridad de la información.

En el mismo ámbito, una política BYOD es considerada como un componente crítico dentro de un esquema BYOD y por este motivo es importante que se delimiten los ámbitos de responsabilidad tanto de la empresa así como del empleado como propietario del dispositivo.

Así, una primera recomendación es que exista una autorización para BYOD con la cual el empleado acepte el uso y participación de un esquema de este tipo, con lo cual la empresa se respalda en casos de pérdida, robo, borrado o en aquellos casos en los cuales sea necesario garantizar la seguridad de la información o incluso cuando se requiera confiscar el mismo.

En segunda instancia es importante garantizar la confidencialidad de la data corporativa, la cual debe diferenciarse de la información personal sin que ello implique husmear en la vida personal del propietario del dispositivo.

Por otra parte (Cavoukian, 2013) sugiere que los componentes esenciales para establecer una política BYOD pueden contemplar algunas de las siguientes consideraciones y criterios específicos contemplados en la tabla 5.

Tabla 5. Consideraciones y criterios específicos para una política BYOD.

CONSIDERACIONES	CRITERIOS ESPECÍFICOS
Seguridad de la información	
Protección de datos	Definir métodos de acceso y aplicaciones a los que accederá cada segmento de usuario.
Confidencialidad	Definir repositorio de data corporativa y manejo de la pérdida de datos.
Propiedad	Definir responsabilidad corporativa ó individual.
Viabilidad de monitoreo / rastreo	Definir actas para manejo de equipos, servicios y aspectos financieros.
Qué hacer cuando empleado renuncia.	Definir riesgos y despliegue de MDM.
Evaluar seguridad en redes inalámbricas.	

Fuente: Adaptado de (Cavoukian, 2013)

Con las consideraciones y criterios específicos mencionados anteriormente se hace necesario incorporar una arquitectura BYOD basada en políticas que según Garba, (Bello, Armarego, & Murray, 2015) proponen que está constituida por tres capas y será tomada como referencia para la propuesta del presente proyecto de tesis. Dicha arquitectura se muestra a continuación en la figura 23.

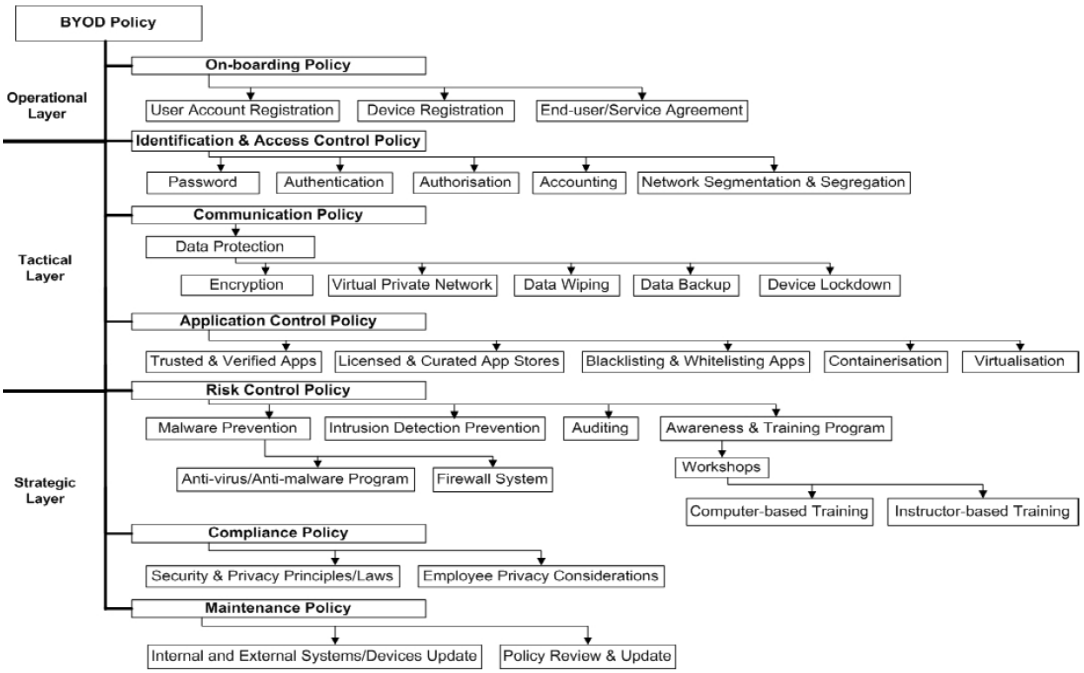


Figura 23. Arquitectura de política BYOD.

Fuente: (Bello, Armarego, & Murray, 2015, pág. 193)

2.6.4 CISCO y BYOD

La marca propietaria Cisco Systems , Inc. se ha constituido como el líder en soluciones integrales de comunicación de datos, video y voz para empresas pequeñas, medianas, grandes e incluso ISP's sean públicas o privadas a nivel mundial.

Parte importante de su portafolio han sido aquellos productos enfocados en integrar soluciones de movilidad y seguridad para redes inalámbricas corporativas suministrando hardware y software dedicado de altas prestaciones como por ejemplo Wireless Lan Controller, Cisco Identity Services Engine, Cisco Mobility Services Engine, Cisco MERAKI que entre otras, sus funciones principales convergen para dotar de seguridad y movilidad al segmento laboral que demanda dichos aspectos.

Como se ha explicado en párrafos anteriores, la tendencia empresarial BYOD ha sido la preocupación de muchas empresas y Cisco ha contemplado un completo sistema de gestión

de movilidad mediante una arquitectura de acceso seguro unificado que provee seguridad y control de dispositivos en redes sin borde dentro de las actuales tendencias empresariales como BYOD; entendiéndose que una red sin borde o sin límites es una concepción donde la infraestructura de red corporativa no distingue dispositivos confiables y no confiables.

2.6.4.1 Cisco Identity Service Engine

Según (Woland & Redmon, CCNP Security SISAS 300-328 Official Cert Guide, 2015), definen a Cisco ISE como una herramienta de gestión de políticas de seguridad y a su vez es componente clave de la arquitectura de acceso seguro de Cisco.

Un esquema BYOD demanda de tres capas de seguridad basadas en políticas que refuerzan la gestión de dispositivos confiables y no confiables, incluso demanda de mecanismos que procuren garantizar métodos efectivos de control de acceso para dichos dispositivos.

En este sentido, Cisco ISE es un componente crítico que le provee a la empresa capacidades para manejar esquemas BYOD mediante la implementación de políticas de seguridad a la medida, sin embargo aunque no posee funciones para administrar dispositivos móviles está compuesto por dos elementos que le proveen una visión completa de la red: información de contexto e información de identidad que en conjunto permiten crear políticas de seguridad pormenorizadas.

La información de contexto refiere aspectos afines a: quién se conectó a la red, donde se conectó, qué software utilizó, cuándo se conectó y cómo lo hizo. Dicha información de contexto es obtenida mediante el uso de funciones como acceso para invitados, perfilamiento, postura, etc.

Por otra parte, la información de identidad está enfocada en suministrar los datos del usuario como: ID, nombres, apellidos, mail corporativo, cargo, etc. y datos del dispositivo como: sistema operativo, software instalado, dirección física, entre otros, mediante el uso de mecanismos como 802.1x, VPN, RADIUS, Web Authentication (CWA / LWA), Mac Address Bypass, entre otros.

A continuación, la figura 24 muestra la arquitectura de Cisco ISE y los subcomponentes que lo constituyen.

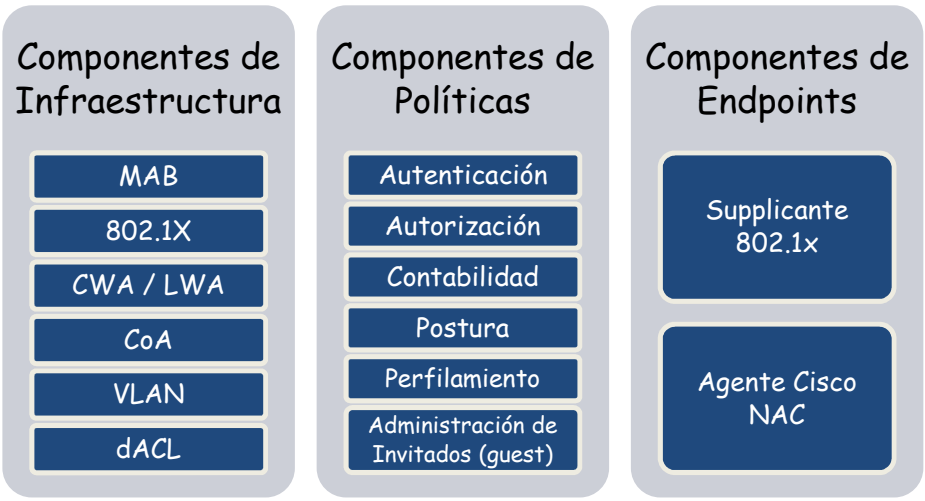


Figura 24. Arquitectura de componentes de Cisco ISE.

Fuente: Adaptado de (Woland & Heary, 2013)

Dentro de un esquema BYOD, es importante clasificar a los dispositivos que se conectan a la red corporativa, lo que implica que dichos dispositivos cumplan con ciertos requisitos y procesos para que puedan hacerlo. Entre los principales requisitos a cumplir están por ejemplo, tener el dispositivo móvil actualizado, disponer de un antivirus con las últimas definiciones de virus, contar con aplicaciones de fuentes certificadas, etc.

Uno de los procesos que un dispositivo debe cumplir para pertenecer a un esquema BYOD es el On-boarding o abordamiento mismo que se puede ejecutar desde dos escenarios: el

primero denominado on-boarding BYOD en el que con Cisco ISE como gestor de políticas de seguridad garantiza que un dispositivo móvil tenga acceso a la red luego de ejecutar de manera exitosa un proceso de registro, asignación de certificado al dispositivo y configuración del suplicante propio del terminal.

Cabe destacar que desde el punto de vista de capa física, el dispositivo móvil previamente debe estar conectado a un esquema de SSID simple o doble, en cuyo caso la única diferencia está en que en el esquema de SSID simple se hace presente un CoA o cambio de autorización que en pocas palabras significa que el nivel de acceso con el que el dispositivo móvil se registra, cambia para que dicho nivel de acceso posteriormente sea más elevado. La figura 25 muestra el proceso de on-boarding BYOD mediante SSID simple.

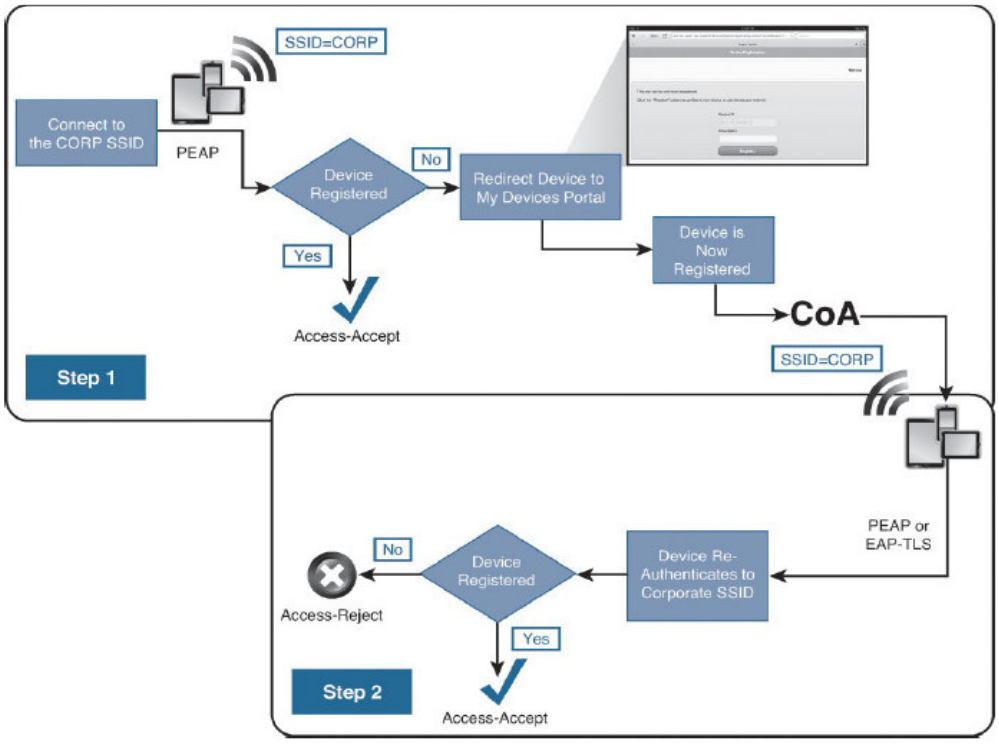


Figura 25. Proceso de On-boarding mediante Cisco ISE y SSID simple.

Fuente: (Woland & Redmon, CCNP Security SISAS 300-328 Official Cert Guide, 2015, pág. 548)

Por otra parte el on-boarding MDM contempla el uso de un sistema MDM en cuyo caso se inicia con el registro, instalación del agente MDM y mejoramiento de las políticas del terminal el mismo que es automatizado.

El profiling o perfilamiento por otra parte, es un mecanismo que permite a Cisco ISE detectar y clasificar a los dispositivos finales en función de las características detectadas y procurando hacerlos coincidir con perfiles de dispositivos previamente creados. En esencia el perfilamiento es utilizado por ejemplo en equipos que no poseen un suplicante que maneje el estándar 802.1x, por otra parte el perfilamiento también permite definir políticas que diferencian el nivel de acceso a red.

3 CAPITULO III: DETERMINACIÓN DE SITUACIÓN ACTUAL RED INALAMBRICA SRI BASADA EN WIPS Y PROPUESTA DE MEJORA.

3.1 Descripción de la "Empresa Pública de Recaudación de Impuestos".

La Empresa Pública de Recaudación de Impuestos, es una empresa de naturaleza pública que nace el 2 de Diciembre de 1997, que está domiciliada en Quito y que cuenta con 47 oficinas que brindan cobertura a nivel nacional. (Servicio de Rentas Internas [SRI], 2016).

Aunque su función principal es la de recaudar impuestos, con el tiempo ha evolucionado y se ha constituido como una célula económica y social formada por recurso humano que le permite estar al servicio de la sociedad e identificada con ella poniendo a su disposición nuevos productos tecnológicos como Facturación Electrónica, SRI Móvil, servicios en línea, etc, que facilitan el cumplimiento de las obligaciones tributarias y que a su vez trascienden en un beneficio hacia los mismos contribuyentes y hacia el país, así lo refiere (Granja & Vallejo, 2015).

Muestra de la eficiencia en la gestión institucional y la constante innovación tecnológica ha sido el incremento notorio en la recaudación de impuestos desde su creación hasta los últimos años haciendo hincapié en el afianzamiento de la cultura tributaria lo que ha incrementado considerablemente el número de contribuyentes a nivel nacional.

Misión

"Gestionar la política tributaria, en el marco de los principios constitucionales, asegurando la suficiencia recaudatoria destinada al fomento de la cohesión social" (Servicio de Rentas Internas [SRI], 2016).

Visión

"Ser al 2019, una institución reconocida por su alto grado de innovación y calidad de servicios dirigidos a la ciudadanía, facilitando el cumplimiento tributario con el fin de mejorar la contribución tributaria y reducir la evasión y elusión fiscal" (Servicio de Rentas Internas [SRI], 2016).

Objetivos Estratégicos

A continuación se presentan los objetivos estratégicos que refiere (Servicio de Rentas Internas [SRI], 2016) en su página oficial.

- Incrementar el cumplimiento voluntario a través de la asistencia y habilitación al ciudadano.
- Incrementar la efectividad en los procesos legales, de control y de cobro.
- Incrementar las capacidades y conocimientos de la ciudadanía acerca de sus deberes y derechos fiscales.
- Incrementar la Eficiencia Operacional en el SRI.
- Incrementar el uso eficiente del presupuesto en el SRI.
- Incrementar el desarrollo del talento humano en el SRI.

3.2 Análisis Situación Actual (confidencialidad)

Se aclara que para determinar la situación actual de la red inalámbrica de la "Empresa Pública de Recaudación de Impuestos" basada en WIPS se respetará los principios de confidencialidad y de no divulgación de información que los funcionarios de la institución mantienen con la misma, considerando la ética y moral que los caracteriza.

Por ello es oportuno aclarar que la información presentada en este proyecto de tesis será verídica pero con las restricciones del caso y en lo posible manteniendo en anonimato aspectos como direccionamiento IP, aspectos críticos de seguridad de la información, configuraciones que se encuentren implementadas en ambientes de producción y parámetros adicionales que pongan en algún tipo de riesgo o expongan la infraestructura institucional crítica.

La "Empresa Pública de Recaudación de Impuestos" implementa e innova constantemente su tecnología dotando de herramientas actuales al recurso humano interno y capacitándolo constantemente para crear productos nuevos y brindar servicios a los ciudadanos y con ello cumplir con los objetivos estratégicos institucionales, sobre todo dotándole al contribuyente de facilidades para el cumplimiento de sus deberes tributarios.

Como parte de los servicios brindados a nivel nacional, la "Empresa Pública de Recaudación de Impuestos" ha implementado una infraestructura inalámbrica que se ponen a disposición del contribuyente que visita las diferentes agencias a nivel nacional, permitiéndole una conexión fácil y sencilla hacia internet para que realice revisiones previas, consultas, etc.

Aunque las principales herramientas para la gestión de accesos está basada en un sistema de gestión de identidades vinculado a una plataforma Microsoft que maneja el Directorio Activo institucional, existen otras plataformas propietarias para la gestión de conectividad

cableada e inalámbrica interna que están dedicas a manejar entre otros aspectos la seguridad de su infraestructura.

En este sentido la situación actual de la red inalámbrica se la pretende definir mediante la descripción de los siguientes componentes:

- Arquitectura de la infraestructura que provee el servicio de red inalámbrica a contribuyentes.
- Características relevantes de los esquemas de seguridad implementados.

Finalmente, la "Empresa Pública de Recaudación de Impuestos" cuenta con una plataforma o solución de conectividad inalámbrica muy robusta y eficiente pero existen implementaciones que aun que operan correctamente, necesitan ser mejoradas o afinadas para poner a punto su funcionamiento y con ello garantizar la seguridad de la red inalámbrica para que cumpla con su objetivo sin comprometerla con intentos de acceso no autorizado en el entorno inmediato a las cuales está expuesta por la ubicación geográfica de sus agencias en las cuales se provee dicho servicio.

3.2.1 Arquitectura de la Red Inalámbrica Institucional

La solución de conectividad inalámbrica que la "Empresa Pública de Recaudación de Impuestos" actualmente tiene, provee un servicio gratuito de acceso a internet para usuarios externos (contribuyentes) que visitan las distintas agencias y provee acceso a la red de datos para los usuarios internos (funcionarios).

La solución de conectividad mediante la cual se gestiona o administran a dicha infraestructura es propietaria de la marca CISCO, mantiene un esquema CUWN "Cisco Unified Wireless Network" en la cual su CORE está implementado en el DATACENTER

principal, su DISTRIBUCIÓN y ACCESO en cada una de las oficinas a nivel nacional, sin embargo la arquitectura está compuesta por los siguientes componentes:

- Wireless Control System – WCS / Cisco Prime Infraestructure – PI
- Mobility Service Engine – MSE
- Cisco Identity Service Engine – ISE (Radius Server)
- Wireless LAN Controller – WLC
- Access Points – AP

La figura 26 muestra claramente un diagrama topológico obtenido a la fecha de realización del presente proyecto de tesis, de los principales componentes que integran la infraestructura de red de la "Empresa Pública de Recaudación de Impuestos" en donde resaltan los componentes anteriormente descritos.

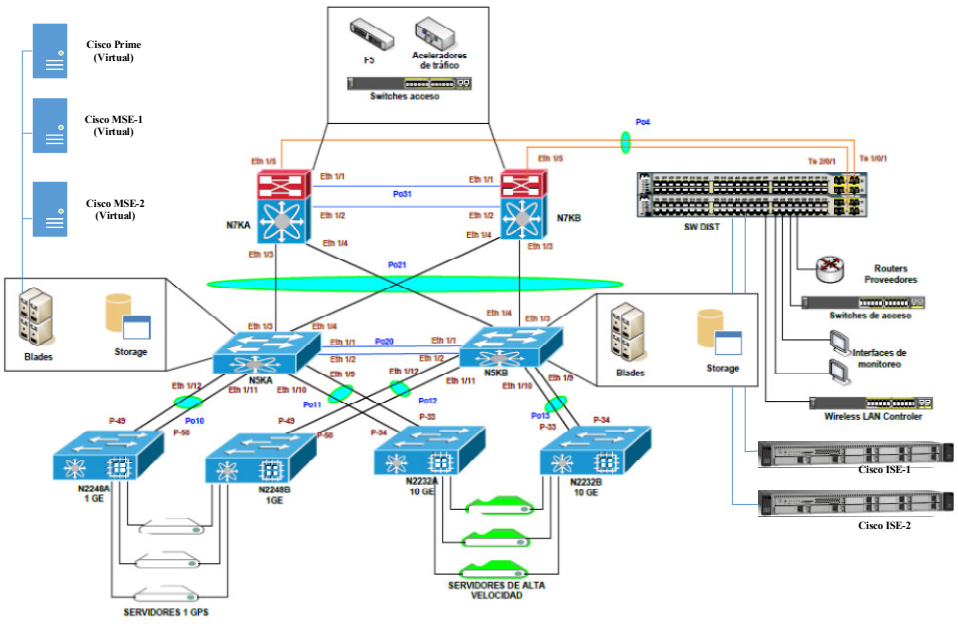


Figura 26. Diagrama topológico principales componentes infraestructura.

Fuente: "Empresa Pública de Recaudación de Impuestos"

El esquema CUWN "Cisco Unified Wireless Network" implementado así como los componentes de dicha arquitectura y la interacción que mantienen se puede apreciar de mejor manera a continuación en la figura 27.

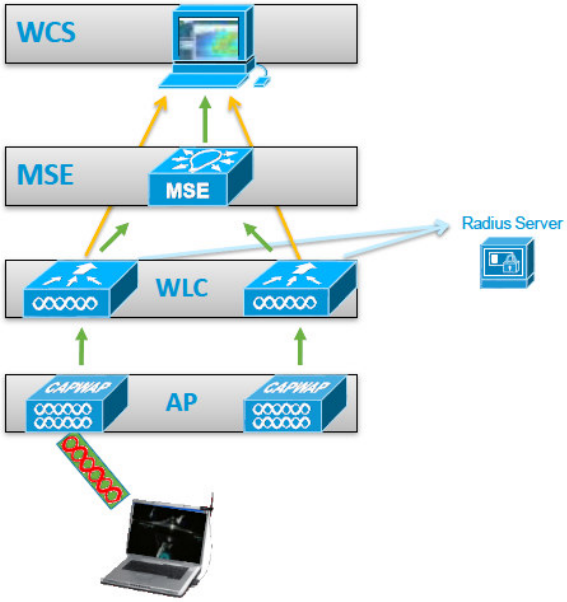


Figura 27. Arquitectura Red Inalámbrica Institucional.

Fuente: "Empresa Pública de Recaudación de Impuestos"

3.2.1.1 Cisco Prime Infrastructure

La marca propietaria CISCO define a este componente como critico por que se constituye como una herramienta para administración de red que mediante su interfaz gráfica integrada brinda posibilidades de monitoreo, aprovisionamiento, optimización y troubleshooting tanto para redes cableadas como para redes inalámbricas. Se debe mencionar que Cisco PI como también se lo conoce es una evolución de la anterior plataforma de administración llamada Wireless Control System que principalmente tenía las mismas funciones que su sucesor.

En este sentido la “Empresa Pública de Recaudación de Impuestos” cuenta al momento de la realización del presente proyecto de tesis, con un appliance virtual en su versión 2.2 de Cisco Prime Infraestructure el cual integra la gestión de otros componentes como Cisco Mobility Service Engine, Wireless Lan Controller y Access Points.

Entre otras, sus principales características son:

- Administración centralizada.
- Visibilidad de aplicación.
- Administración para colaboración móvil.
- Visualización centralizada de redes distribuidas.
- Soporte para redes cableadas e inalámbricas.
    - Mapas de topología de red.
    - Mapas y reportes mejorados para redes wi-fi.
    - Soporte para IPv6.

En el ámbito inalámbrico resaltan las siguientes características:

- Soporte para estándar 802.11ac.
- Soporte para mapas de siguiente generación.
- Integración de mapas con Access points.
- Localización de dispositivos móviles.

Es importante mencionar que como parte de sus funciones principales, Cisco Prime Infrastructure provee esquemas de seguridad inalámbrica como servicio, por ejemplo la detección y prevención de intrusiones.

Aunque su implementación en la "Empresa Pública de Recaudación de Impuestos" es más o menos reciente, no se han aprovechado al máximo sus funcionalidades, lo cual genera una necesidad interna a fin de conseguir mejores prestaciones y garantizar la seguridad de la red inalámbrica aprovechando sus funcionalidades.

3.2.1.2 Cisco MSE - Mobility Service Engine

Es una plataforma modular que se integra con Cisco PI (Prime Infrastructure) para proveer dos servicios principales:

- CAS (context aware services)
- wIPS (wireless intrusion prevention system)

El servicio CAS provee la capacidad de ubicar a cualquier dispositivo cableado o inalámbrico en la red. En el caso inalámbrico, hace uso de Wireless Lan Controller y de Access Points desplegados a nivel nacional.

El servicio wIPS en cambio, provee la capacidad de prevenir amenazas mediante el monitoreo, clasificación, alarmas y remediación.

En el anexo 1, se encuentra un resumen de las principales características de Cisco MSE extraídas del datasheet del fabricante.

La "Empresa Pública de Recaudación de Impuestos" al momento de la realización del presente proyecto de tesis cuenta con una plataforma Cisco MSE en su versión 8.0.110.0

conformado por dos appliance's virtuales en donde el servicio wIPS está siendo administrado por el MSE 02 y aunque se encuentra activado, no está configurado, por lo cual, cualquier tráfico o comportamiento detectado al momento de una conexión inalámbrica es mostrado como un posible ataque lo cual genera alertas erráticas, los logs y la estadística no es real o confiable.

La figura 28 muestra la interfaz gráfica de Cisco PI en donde se puede apreciar a los dos appliance Cisco MSE en donde por otra parte el MSE 01 tiene activado los servicios de Context Aware, Mobile Concierge, entre otros que como se mencionó anteriormente son utilizados para localización de dispositivos en la red institucional pero sin embargo no son motivo del presente proyecto se tesis.

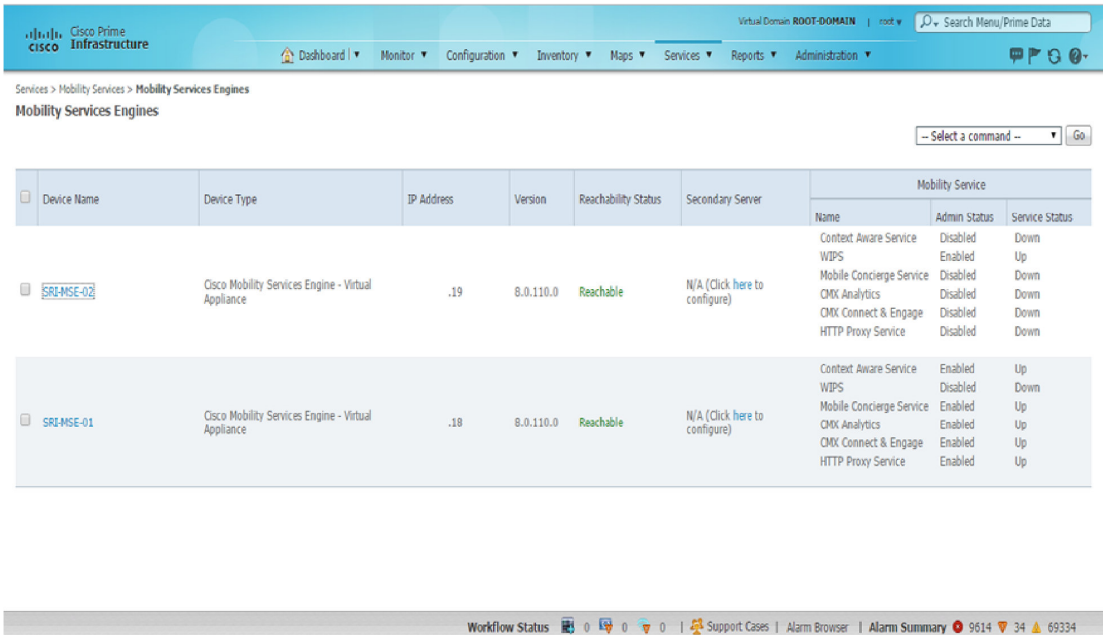


Figura 28. Cisco MSE.

Fuente: "Empresa Pública de Recaudación de Impuestos".

3.2.1.3 Cisco Identity Service Engine

Cisco ISE como también se lo denomina, es una plataforma de administración de políticas de seguridad que le provee a la empresa la posibilidad de asegurar su infraestructura informática incluso mediante la recolección de información contextual en tiempo real. Dicha información contextual se refiere a aspectos como: quién, como, donde se efectuó una conexión y dependiendo de ello se aplica un perfilamiento que le brinda un nivel de acceso. En el anexo 2, se podrá revisar un resumen de las principales características y beneficios de Cisco ISE, extraídos del datasheet del fabricante.

Al momento de realizar el presente proyecto de tesis, Cisco ISE es implementado en su versión 1.3 de la plataforma. Es importante resaltar que Cisco ISE es en esencia un servidor RADIUS que utiliza bases de datos internas denominadas "identity store" o fuentes externas como Active Directory, LDAP, etc, para realizar los procesos de autenticación y autorización.

Como se puede observar en la topología general anteriormente presentada, la "Empresa Pública de Recaudación de Impuestos" al momento de la realización del presente proyecto de tesis cuenta con la plataforma Cisco ISE implementada mediante dos appliance físicos configurados en modo HA (High Availability) o alta redundancia, escenario en el cual uno de ellos opera en modo primario y el otro en modo secundario, es decir si por alguna razón existe indisponibilidad del nodo primario, el nodo secundario entrará en operación considerando que constantemente existe una sincronización de sus configuraciones.

3.2.1.4 Wireless Lan Controller

También denominado WLC por sus siglas, es el corazón de una solución de red inalámbrica unificada pues análogamente a la creación de un router con el fin de interconectar redes, el WLC es creado con el objetivo de proveer un solo punto de administración y gestión de toda una red inalámbrica incluyendo sus Access points.

El WLC se define como una plataforma de administración de infraestructura inalámbrica de alto desempeño que está constituido con hardware de seguridad para entornos 802.11 empresariales de gran demanda.

Al momento de la realización del presente proyecto de tesis, el WLC está implementado con un clúster de dos equipos físicos marca Cisco modelo 5508 en modo de alta redundancia. Se puede apreciar en la figura 29 que el WLC primario se encuentra en la versión 8.0.121.0.

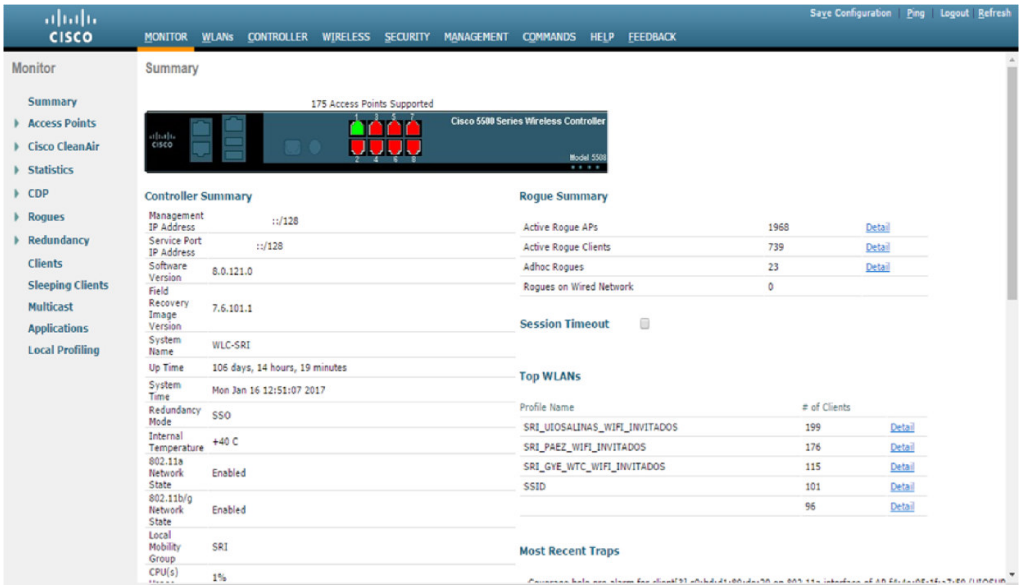


Figura 29. Interfaz WLC primario.

Fuente: "Empresa Pública de Recaudación de Impuestos"

Actualmente la "Empresa Pública de Recaudación de Impuestos" cuenta con licenciamiento aproximadamente para 175 Access Points, sin embargo al momento de la realización del presente proyecto de tesis se encuentran desplegados 149 access points a nivel nacional ubicados estratégicamente en cada piso de las distintas agencias así como en aquellas que disponen de espacios para atención al cliente.

Para que el WLC pueda centralizar la administración de los access points, éstos deben estar en modo lightweight permitiéndole así configurar íntegramente todos sus parámetros de seguridad.

3.2.1.5 Access Points

También definidos como WAP "wireless access points" o AP son dispositivos que permiten interconectar equipos de red que cuenten el hardware apropiado para interceptar o interpretar el estándar 802.11.

Dichos AP's están funcionando en modo Lightweight, que les permite ser gestionados desde un solo punto, que como se había mencionado en el ítem anterior es el WLC.

Los AP's con los que cuenta la institución son en su totalidad de marca CISCO y están desplegados a nivel nacional. En la tabla 6, presentada a continuación se puede apreciar de mejor manera la cantidad de acuerdo al modelo.

Tabla 6. Cantidad de AP's por modelo "Empresa Pública de Recaudación de Impuestos"

MODELO AP	CANTIDAD
AIR-CAP3702I-A-K9	118
AIR-CAP3602I-A-K9	12
AIR-LAP1141N-A-K9	9
AIR-LAP1041N-A-K9	10
TOTAL	149

Fuente: "Empresa Pública de Recaudación de Impuestos"

Se debe discriminar que un grupo de AP's cuentan con un módulo adicional denominado WSM "Wireless Security Module" compatible con los AP's de modelo 3600 y 3700. Dichos Access points están distribuidos de manera estratégica a nivel nacional principalmente en la agencias que brindan el servicio de atención al contribuyente como se puede observar en la tabla 7.

Tabla 7. Distribución Módulos WSM "Empresa Pública de Recaudación de Impuestos".

UBICACIÓN	AIR-RM3000M	UBICACIÓN	AIR-RM3000M
PAEZ	3	**SANTA ELENA**	1
TUMBACO	1	**TUFIÑO**	2
AMBATO	2	**PIÑAS**	1
SANTA ROSA	1	**STA. CRUZ**	1
TULCAN	1	**QUEVEDO**	1
SANGOLQUI	1	**ESMERALDAS**	1
AMAZONAS	1	**RIOBAMBA**	1
SALINAS	1	**RIOBAMBA NORTE**	1
IBARRA	1	**SAN CRISTOBAL**	1
STO. DOMINGO	1	**BAÑOS**	1
SUCUMBIOS	1	**MILAGRO**	1
GYE GARZOTA	2	**COCA**	1
GYE CALIFORNIA	1	**LATACUNGA**	1
GYE WTC	2	**LAMANA**	1
GYE SUR	1	**MACAS**	1
AZOGUES	1	**AG. SUR**	2
GUARANDA	1	**TRONCAL**	1
CUENCA	1	**BABAHOYO**	1
PUYO	1	**LOJA**	1
MANTA	1	**ZAMORA**	1
CHONE	1		
TOTAL			48

Fuente: "Empresa Pública de Recaudación de Impuestos".

En ese punto es importante aclarar que los Access points desplegados a nivel nacional están suministrando o difundiendo varios SSID que facilitan la conectividad tanto para los funcionarios (usuarios internos) así como como para los contribuyentes (usuarios externos).

Considerando entonces la ventaja de una administración centralizada que proporciona el WLC, se analizará la seguridad en el SSID etiquetado como "FUNCIONARIOS" y del SSID etiquetado como "SRI_CIUDADANO" al servicio de contribuyentes.

3.2.2 Esquemas de seguridad implementados en la red Inalámbrica

Como se menciona en el punto 3.2.1.5 Access Points, el presente proyecto de tesis se enfocará en analizar la seguridad en la red inalámbrica para contribuyentes como para funcionarios de la agencia principal de la "Empresa Pública de Recaudación de Impuestos". Los SSID de cada una de estas redes mantienen una configuración que procura garantizar conectividad y seguridad. Por otra parte está el hecho de que cierta cantidad de AP's de la institución incorporan un módulo WSM mencionado anteriormente pero que no está correctamente configurado para desempeñar su funcionalidad.

3.2.2.1 SSID para usuarios internos y externos.

Por razones de confidencialidad no se puede poner de manifiesto parámetros técnicos que pongan en algún tipo de riesgo la seguridad de la infraestructura institucional como por ejemplo el nombre del SSID que permite la conectividad a la red inalámbrica interna de los funcionarios, por cuanto parte de su configuración está planteada para que su SSID no se difunda, es por ello que se utilizará el nombre de "FUNCIONARIOS" para referirse al SSID de dicha red y el SSID para contribuyentes será al que se utiliza al momento de la realización del presente proyecto de tesis denominado "SRI_CIUDADANO".

Es relevante recordar que toda la configuración a nivel de AP's y SSID así como grupos de AP's son administrados por el WLC y también por Cisco Prime Infrastructure.

Así, la red con SSID "FUNCIONARIOS" mantiene un nivel de seguridad elevado que se puede apreciar en la figura 30, en donde se evidencia que existe un primer nivel de seguridad que consiste en ocultar el SSID o dicho de otra manera el Broadcast SSID se encuentra deshabilitado.

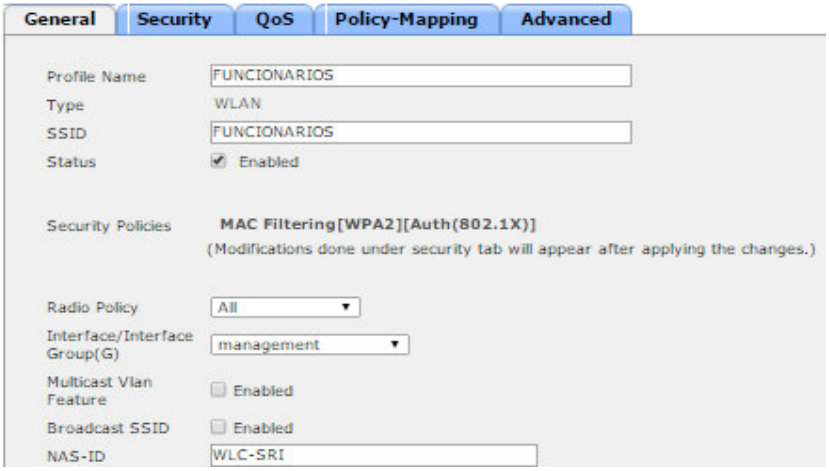


Figura 30. Configuración General SSID "FUNCIONARIOS"

Fuente: Autor.

A nivel de capa 2 la seguridad implementada contempla por una parte el uso del mecanismo no estandarizado *Mac Filtering* para validar la dirección física de los equipos a conectarse, adicionalmente cuenta con el mecanismo WPA/WPA2 con AES y 802.1x como mecanismo de autenticación que denota la existencia de un servidor RADIUS que para el presente caso de estudio, dicho servidor está representado por la plataforma Cisco ISE.

Dicha configuración de puede evidenciar a continuación en la figura 31 en donde se puede resaltar el mejor nivel de encriptación que maneja el estándar WPA2/AES.

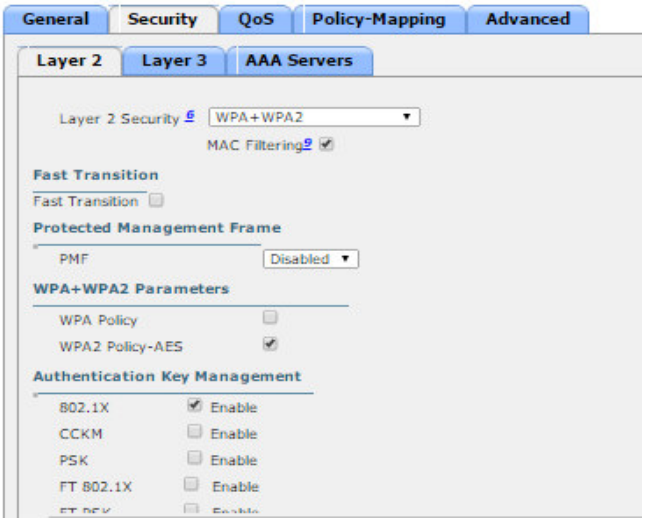


Figura 31. Configuración seguridad capa 2 SSID "FUNCIONARIOS"

Fuente: Autor.

La autenticación mediante 802.1x implica el uso de un servidor RADIUS el cual está direccionado en la pestaña "AAA Servers" como se puede apreciar a continuación en la siguiente figura 32.

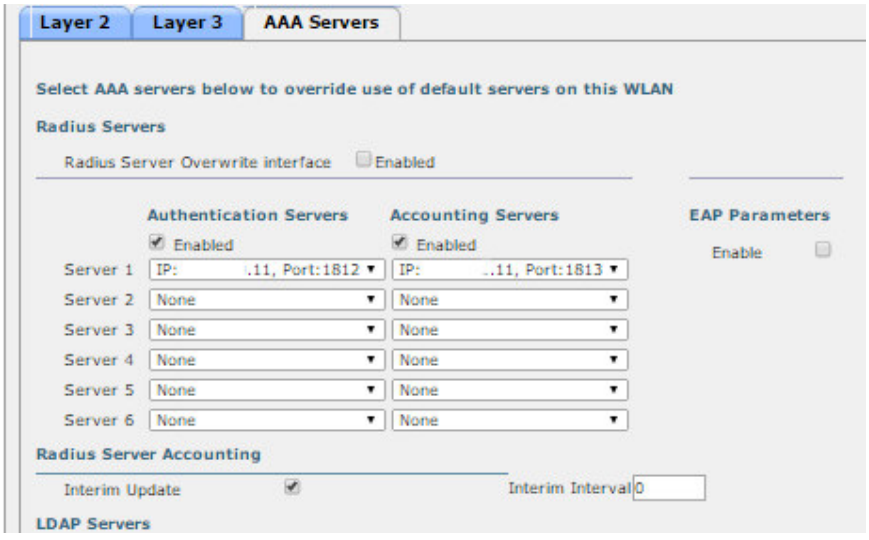


Figura 32. configuración RADIUS SSID "FUNCIONARIOS"

Fuente: Autor.

En este punto se puede concluir que la red con SSID “FUNCIONARIOS” cuenta con algunos niveles de seguridad que la hacen más robusta, sin embargo es oportuno mencionar que a nivel institucional no existe una política que regule el acceso a dicha red inalámbrica, para usuarios externos por ejemplo.

Por otra parte, la red de contribuyentes con SSID “SRI_CIUDADANO” cuenta con una configuración mucho más simple por así decirlo, una de las principales razones de ello es que en su originalmente fue planificada para que brinde facilidad de conexión al contribuyente, sin embargo, a su vez, representa una seria vulnerabilidad. La figura 33, muestra su configuración general.

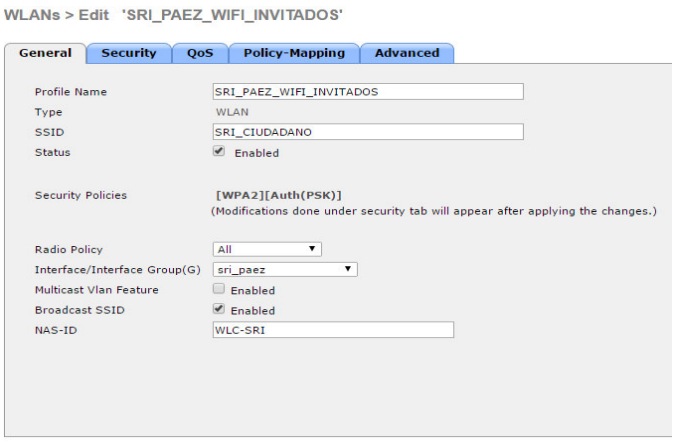


Figura 33. Configuración General SSID “SRI_CIUDADANO”

Fuente: Autor.

En este sentido, aunque la red no está oculta, a nivel de capa 2 su configuración es idéntica a la red “FUNCIONARIOS” con la diferencia de que ésta no hace uso del mecanismo MAC Filtering que como ya se había mencionado, funciona como una validación previa comparando la dirección física o MAC Address del cliente inalámbrico contra una BDD interna del WLC que debe ser previamente registrada lo que garantiza el estado de asociación - autenticación.

Algo que se debe resaltar es que aunque dicha red utiliza el mecanismo WPA2/AES, su método de autenticación es PSK que como se había mencionado en el marco teórico, implica el uso de una clave compartida que debe conocer tanto el cliente inalámbrico como la estación, lo que para el criterio de personas mal intencionadas es información relevante para posibles ataques.

En este contexto, la localización geográfica de la agencia de la "Empresa Pública de Recaudación De Impuestos" que es motivo del presente proyecto de tesis, está en las inmediaciones de una zona altamente poblada lo que representa la posibilidad de intentos de acceder sin autorización a los servicios que dicha empresa provee a sus contribuyentes y no descarta posibles ataques maliciosos.

La figura 34 muestra la configuración a nivel de capa 2 del SSID "SRI_CIUDADANO" administrada por el WLC.

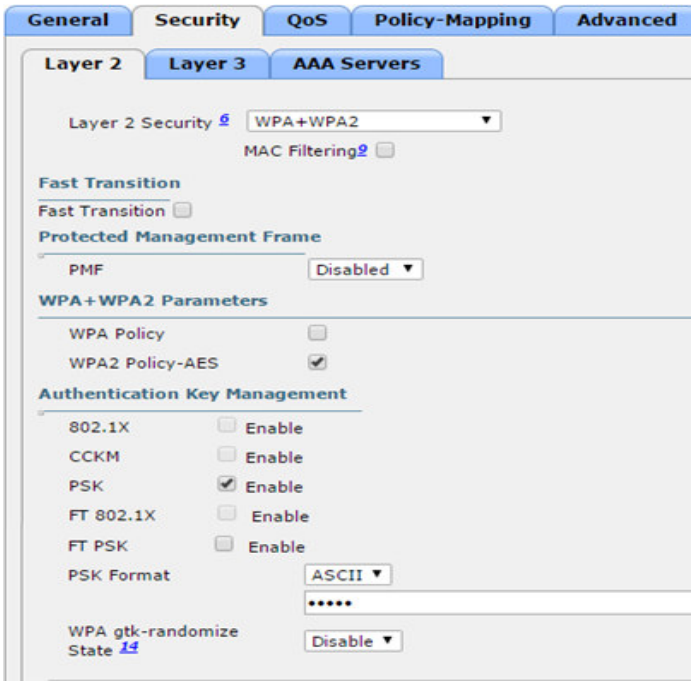


Figura 34. Configuración seguridad capa 2 SSID "SRI_CIUDADANO"

Fuente: Autor.

3.2.2.2 WIPS en la "Empresa Pública de Recaudación de Impuestos"

El tópico que agrega valor al presente proyecto de tesis, es sin duda cómo un tradicional sistema de prevención de intrusiones se aplica a la tecnología 802.11 que cada vez evoluciona y su ubiquidad crece y se difunde no solo en el ámbito gubernamental. Cisco Prime Infrastructure como ya se definió anteriormente, es una plataforma para administración de red muy completa que incluye la gestión del servicio wIPS mediante políticas, alarmas y notificaciones y que al no contar con una configuración adecuada, sondea todo tipo de tráfico en el entorno inalámbrico e interpreta como ataque eventos como varios intentos de autenticación de parte de un cliente que falló en el ingreso de la clave de acceso, por ejemplo.

El escenario que se analiza al momento de realizar el presente proyecto de tesis es evidente, por cuanto su arquitectura es distribuida y se sabe que existe un licenciamiento wIPS que habilita la utilización del dicho servicio mediante sus AP's, pero necesita ser correctamente configurado y evidenciar que existe un monitoreo de parte de dicha tecnología.

La documentación de la marca CISCO referenciada en el presente proyecto de tesis, resalta que wIPS tiene ventajas pero también tiene limitaciones, mismas que definen los alcances que tiene esta tecnología; una de estas desventajas refiere que Cisco MSE puede ser configurado únicamente desde Cisco Prime Infrastructure. Por otra parte, considerada como una desventaja que particularmente llama la atención es que el perfilamiento wIPS podrá ser aplicado únicamente a un WLC lo que a su vez implica que todos los AP's que están siendo gestionados por dicho WLC comparten el mismo perfil de monitoreo, sin embargo dicho monitoreo puede ser aplicado de manera diferenciada basado en filtros como: dispositivos internos, dispositivos externos, uno o varios SSID.

Bajo las consideraciones de arquitectura a la cual responde el presente análisis, se planteó una metodología de trabajo que permitiría rescatar los parámetros más relevantes de las configuraciones de los AP's que manejan la funcionalidad wIPS y diferenciarlos de los que no.

En tal virtud, el primer paso fue realizar una confirmación de los AP's con los que cuenta la agencia que es objeto del presente análisis para posteriormente determinar cuáles son los AP's que cuentan con el módulo WSM y finalmente determinar que configuración de seguridad mantienen.

Es así que se ha determinado en primera instancia que la agencia principal de la "Empresa Pública de Recaudación de Impuestos" cuenta con el servicio de atención al contribuyente en donde se provee el servicio de internet inalámbrico. Dicha agencia cuenta con nueve AP's CISCO de los cuales es necesario conocer cuántos permiten un monitoreo mediante el módulo WSM.

Para este objetivo, mediante una conexión SSH o telnet hacia el AP, se permite acceder a la CLI "command line interfaz" de dicho Access point en el cual el comando "show inventory" muestra un inventario del hardware que incluye. Esto se puede evidenciar en la figura 35 en donde claramente se observa algunos parámetros importantes como por ejemplo; que es un AP Cisco Aironet 3700 series, su modelo exacto es AIR-CAP3702I-A-K9 y lo más relevante es que dicho AP cuenta con un módulo WSM modelo AIR-RM3000M para realizar monitoreo wIPS.

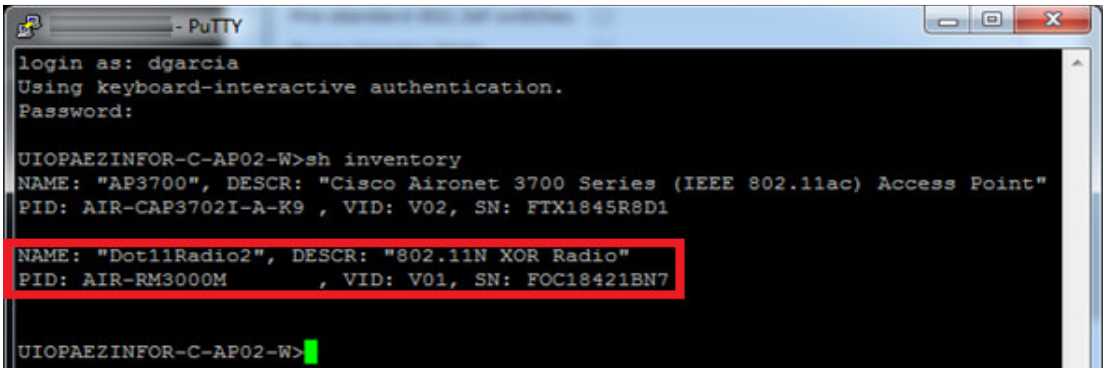


Figura 35. Validación de módulo WSM en AP Cisco 3700.

Fuente: Autor.

A diferencia de lo anteriormente expuesto, a continuación la figura 36 muestra cuando el AP no dispone de un módulo WSM.

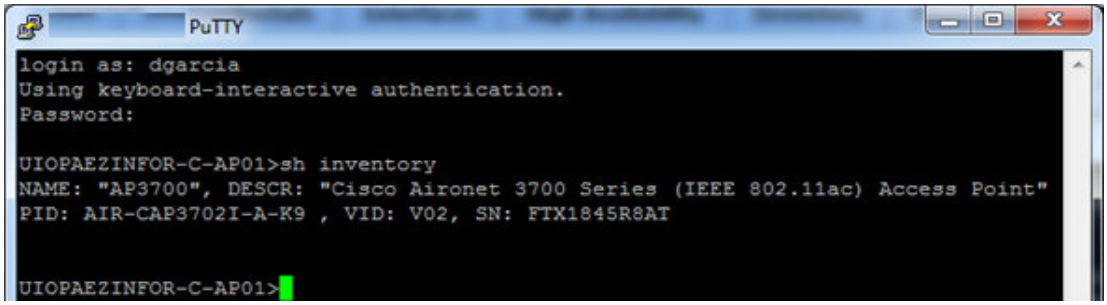


Figura 36. Validación de no disponibilidad módulo WSM en AP Cisco 3700.

Fuente: Autor.

Como resultado de esta validación se determinó que, de los nueve AP's ubicados en la agencia principal de la "Empresa Pública de Recaudación de Impuestos", tres disponen de un módulo WSM y sobre ellos se deberá aplicar una configuración wIPS que registre eventos relacionados a posibles intentos de ataque. Dichos AP's están listados a continuación en la tabla 8.

Tabla 8. Access Points con módulo WSM.

NOMBRE	MODELO AP	MODULO WSM
UIOPAEZINFOR-C-AP02-W	AIR-CAP3702I-A-K9	AIR-RM3000M
UIOPAEZRUC-C-AP02-W	AIR-CAP3702I-A-K9	AIR-RM3000M
UIOPAEZRUC-C-AP01-W	AIR-CAP3702I-A-K9	AIR-RM3000M

Fuente: Autor.

En este contexto el tercer factor a determinar es la configuración específica de seguridad que cada uno de los AP's maneja, sin embargo para efectos explicativos, a continuación se presentará evidencias de la configuración de uno de ellos dejando para la propuesta la configuración completa de cada uno.

A continuación la figura 37, muestra la configuración más relevante de un AP que cuenta con el módulo WSM para monitoreo mediante tecnología wIPS.

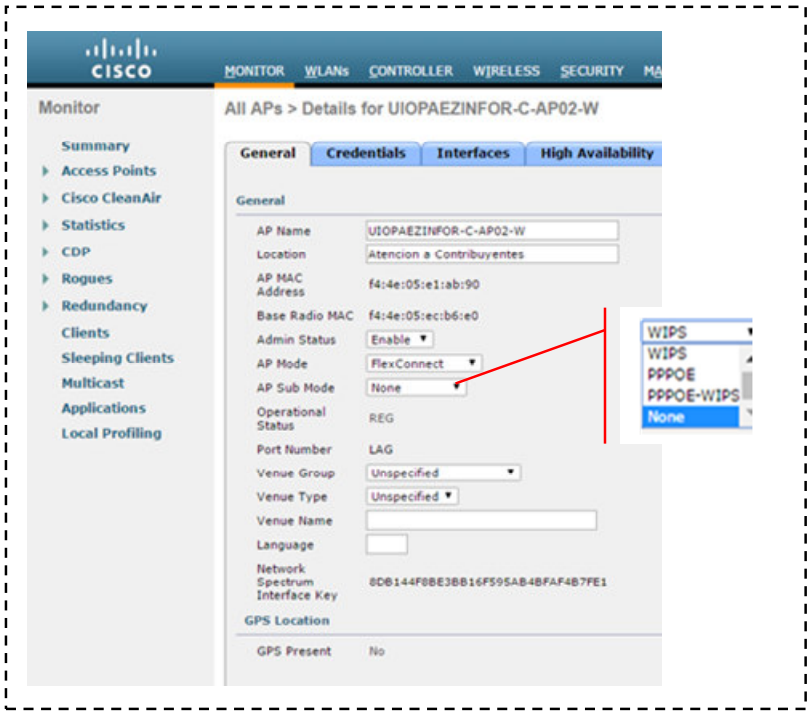


Figura 37. Configuración AP con módulo WSM.

Fuente: Autor.

Como se había mencionado anteriormente, Cisco PI, mediante Cisco MSE administra el servicio wIPS, sus perfiles y su aplicación al WLC y éste último difunde dichos perfiles de monitoreo a todos los AP's. La figura 38, muestra los perfiles creados y como se puede apreciar, está listado el perfil que viene por defecto y un perfil creado para realizar pruebas y que no está siendo aplicado a ningún controlador o WLC.

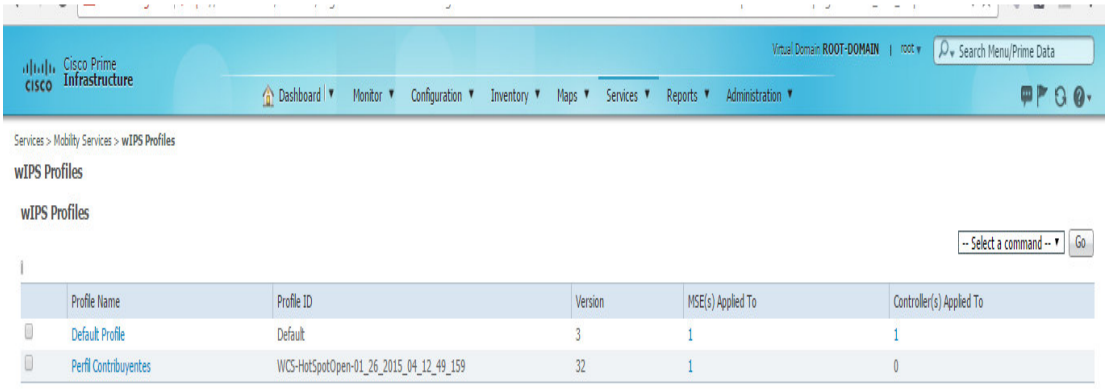


Figura 38. Perfiles WIPS.

Fuente: Autor.

En este punto se puede proyectar un panorama en el cual se cuenta con la tecnología necesaria para maximizar la seguridad de la red inalámbrica pero sin embargo es necesaria una afinación que permita sacar provecho de la misma, resaltando que en Cisco PI necesita la definición de perfiles wIPS y la reasignación de dichos perfiles a un controlador WLC el cual propagará el perfilamiento a cada uno de los AP's de la infraestructura en base a criterios como Grupo de Dispositivos o SSID.

3.3 Propuesta de Mejora

Luego de determinar y analizar la situación actual de la red inalámbrica de la "Empresa Pública de Recaudación de Impuestos" se planteará configuraciones que permitan mejorar la seguridad de dicha red enfocándose principalmente en el ámbito más vulnerable que es el servicio ofrecido a los contribuyentes, por cuanto se ha concluido que dicha red es la que menos seguridades posee y es susceptible a posibles ataques principalmente de los sectores aledaños considerando que su ubicación es céntrica y está rodeada por construcciones que albergan hoteles, pequeñas empresas y negocios que proliferan por la creciente demanda de trámites a realizarse en la agencia principal de dicha empresa.

En este sentido la propuesta a plantearse contempla afinar configuraciones en dos componentes de la arquitectura antes mencionada; estos componentes son:

- Cisco Access Point.
- Cisco Prime Infrastructure – Cisco Mobility Services Engine.

Es importante mencionar que las configuraciones serán propuestas para ser ejecutadas desde el entorno gráfico o GUI de cada plataforma analizada a efectos de facilitar la ejecución de las mismas y considerando la versiones vigentes al momento de la realización del presente proyecto de tesis.

3.3.1 Configuración propuesta para Access Points

Para que el Sistema de Prevención de Intrusiones Inalámbrico wIPS funcione correctamente, es necesaria una configuración tanto en Access points así como a nivel del Prime Infrastructure - Cisco MSE. Por este motivo, en esta etapa de la propuesta se tratará en primer lugar la configuración a nivel de aquellos Access points que cuentan con el

módulo WSM para monitoreo wIPS, y su procedimiento es detallado de manera gráfica en el anexo 3.

Como se menciona anteriormente, los AP de CISCO soportan ciertos modos de funcionamiento y con el licenciamiento adecuado a nivel de MSE e incluso sin necesidad de un módulo WSM puede detectar posibles ataques, sin embargo se debe resaltar que en este escenario se obliga al AP a no difundir ningún SSID lo que a su vez requiere incluir un AP exclusivamente para el servicio inalámbrico de datos a diferencia de aquellos AP's equipados con dicho módulo WSM que garantizan ofrecer un desempeño adecuado mientras proveen conectividad a nivel de la red de datos y a la vez realizan un sondeo del entorno inalámbrico.

De acuerdo a la documentación de CISCO la configuración de aquellos AP's que cuentan con el módulo WSM para monitoreo wIPS deben contemplar la siguiente configuración:

- Ap habilitado *Admin Status*.
- Ap en modo FlexConnect (recomendado para ELM AP).
- Ap habilitada la compatibilidad con wIPS.

Para que el servicio wIPS funcione correctamente se debe primeramente deshabilitar temporalmente "Admin Status". Aunque esta configuración también se la puede realizar desde el WLC se la puede realizar desde Cisco Prime Infrastructure.

- En Cisco PI vers. 2.2, en la pestaña *Configuration* se encuentra la opción *Access Points Radios*. Esta opción permitirá desplegar el listado total de AP's. La figura 39 muestra el detalle.

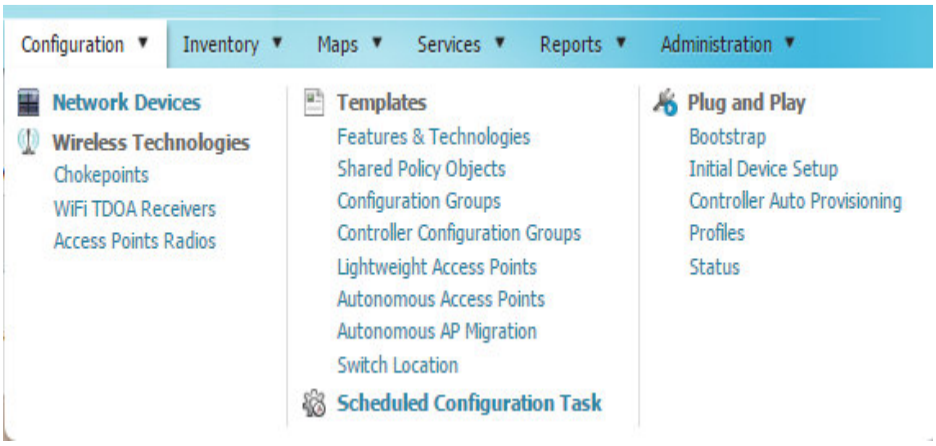


Figura 39. Acceso a Access Points desde Cisco Prime Infrastructure.

Fuente: Autor.

- Del total de AP's se consideraran los detallados en el punto 3.2.2.2 wIPS en la "Empresa Pública de Recaudación de Impuestos" debido a que son aquellos que cuentan con un módulo WSM para monitoreo wIPS, lo cual se puede apreciar a continuación en la figura 40.

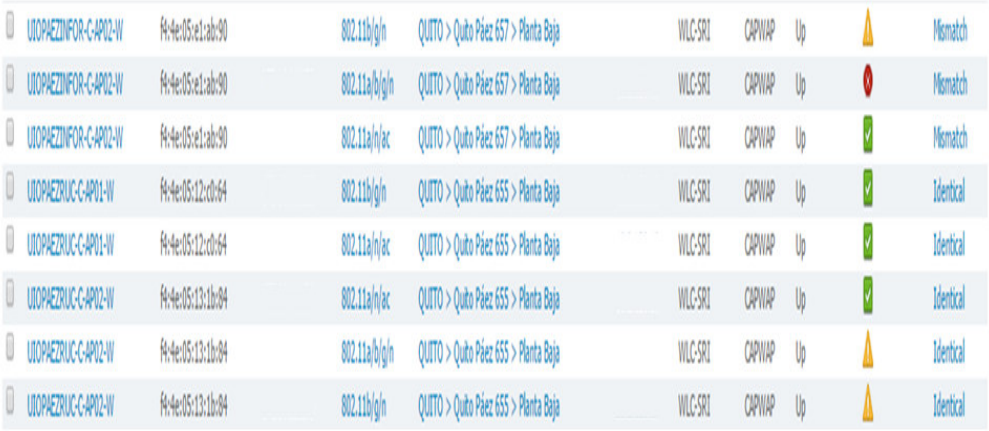


Figura 40. Access points con modulo WSM.

Fuente: Autor.

- La deshabilitación de *Admin Status* se la realiza temporalmente y como paso previo a poner al AP en modo FlexConnect. Este procedimiento se lo realizó seleccionando la casilla *Admin Status* como se puede evidenciar en la figura 41 a continuación.

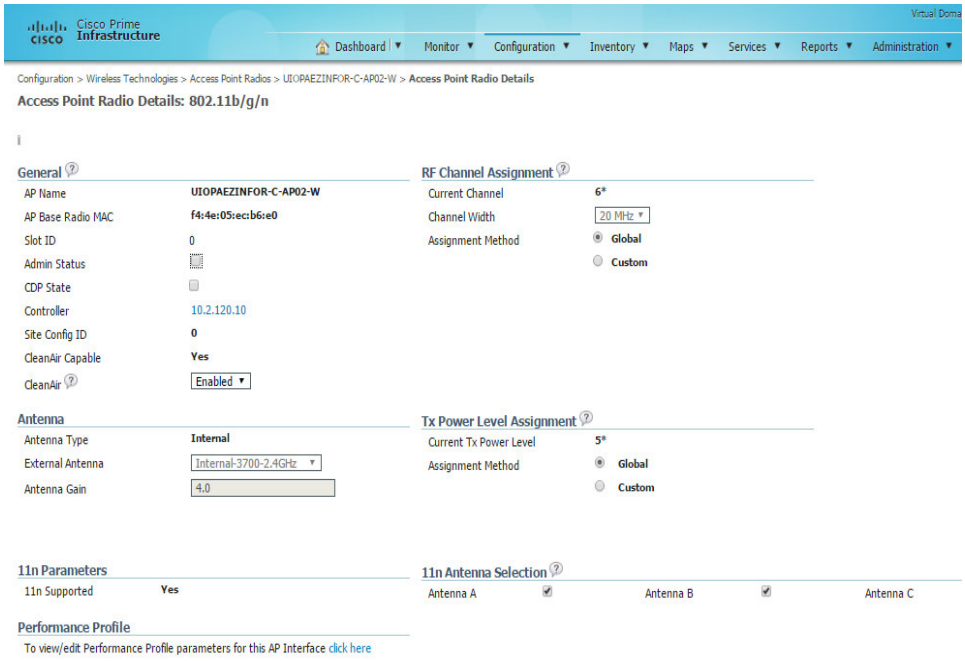


Figura 41. Desactivación temporal Admin status.

Fuente: Autor.

- La habilitación del modo FlexConnect en el AP se consiguió accediendo al AP ahora mediante su nombre de host en donde se habilitó dos parámetros que en esencia ponen al AP en modo FlexConnect dándole autonomía al AP en casos de pérdida de conexión con el WLC y habilitan el sub-modo de operación wIPS como se puede apreciar a continuación en la figura 42.

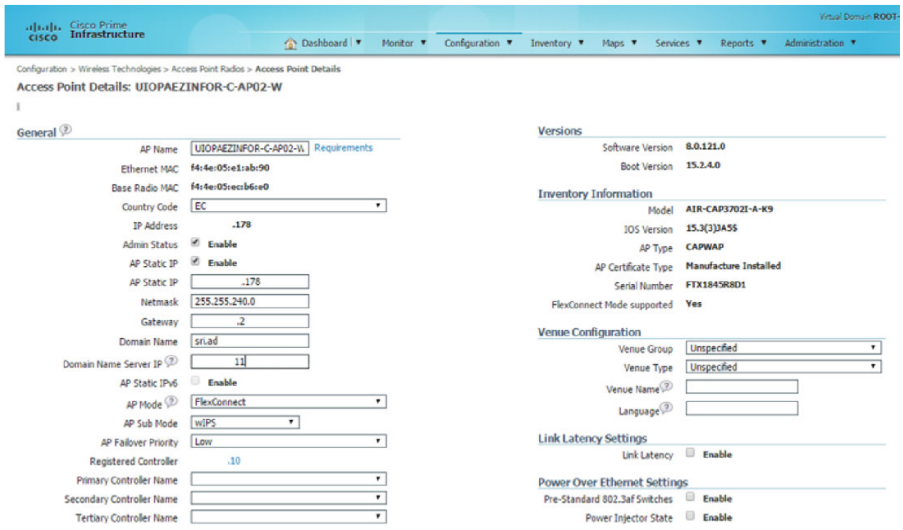


Figura 42. Activación modo FlexConnect y sub-modo wIPS.

Fuente: Autor.

- Finalmente la re-activación de Admin Status deja al AP listo para monitorear el entorno inalámbrico con su módulo WSM el cual enviará los incidentes detectados hacia el componente Cisco MSE para hacer uso de la tecnología wIPS.

3.3.1 Configuración propuesta para Cisco MSE – Cisco Prime Infrastructure

La configuración propuesta a nivel de MSE – Prime Infrastructure contemplará aspectos que permitirán proveer el servicio de monitoreo wIPS. En este sentido es importante mencionar que la tecnología wIPS de Cisco provista como servicio a través de MSE necesita principalmente y a breves rasgos la creación de perfiles, configuración de alarmas y aplicación de un perfil a una controladora para su correcta adopción en cada AP.

A efectos de ejemplificar dicha configuración, los procedimientos realizados se explican a continuación y se los detalla de manera gráfica en el anexo 4.

En este sentido la configuración propuesta intentará inicialmente mostrar la configuración de un perfil wIPS, mismo que como ya se mencionó se encuentra alojado como un servicio dentro de *Mobility Services* en la opción *Services.* A continuación la figura 43 muestra lo mencionado.

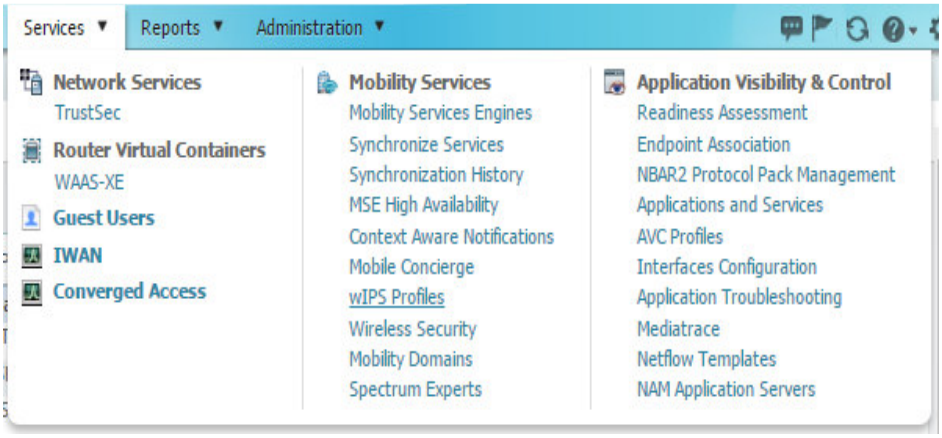


Figura 43. Acceso a configuración de perfiles wIPS.

Fuente: Autor.

- Por defecto Cisco MSE incluye un perfil de monitoreo wIPS el cual está sujeto a modificaciones con el objetivo de que sea adaptado a las necesidades empresariales sin embargo dicho perfil no es aplicado a ningún Wireless Lan Controller. A continuación, en la figura 44 se evidencia los perfiles creados como propuesta. El perfil denominado "PERFIL_CONTRIBUYENTES" fue creado con el objetivo de configurar las políticas de seguridad para la detección de ataques en la red con SSID "SRI_CIUDADANO".

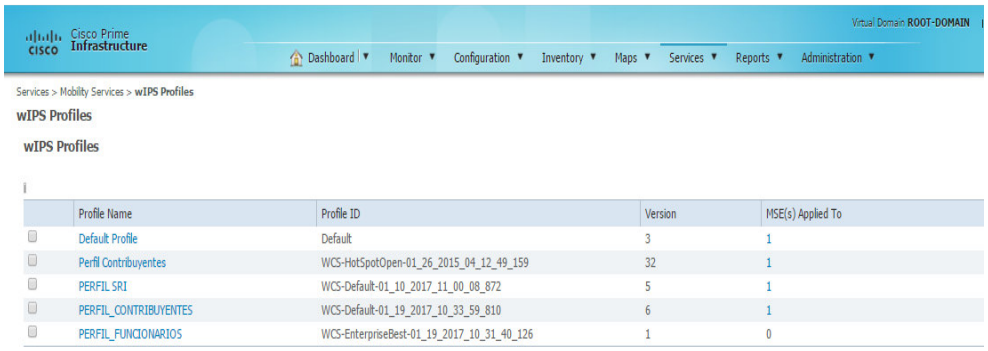


Figura 44. Perfiles wIPS creados.

Fuente: Autor.

- Dentro del proceso de configuración del servicio wIPS está la asignación de *SSID Group List*, configuración que permite definir los SSID a los cuales se realizará el monitoreo. En este sentido se ha creado el grupo denominado "WLAN_CONTRIBUYENTES". A continuación la figura 45 muestra lo comentado.

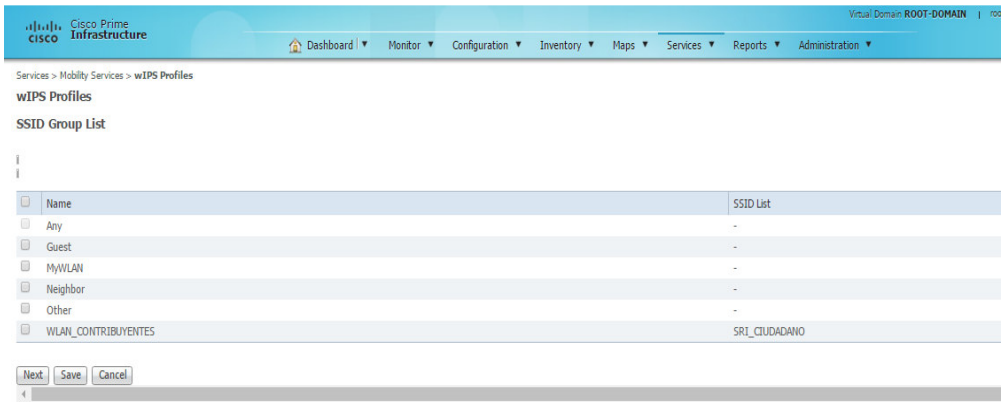


Figura 45. SSID Group List creado para perfil wIPS.

Fuente: Autor.

- El aspecto más relevante de la configuración del servicio wIPS es la activación de las políticas y sus respectivas alarmas que a pesar de que por defecto la plataforma Cisco MSE define configuraciones prestablecidas de acuerdo al entorno de

implementación de una solución unificada inalámbrica es importante destacar que se requiere de una personalización por cuanto esto permitirá enfocar el monitoreo y la detección de intrusiones en función de los esquemas de seguridad implementados a nivel de AP's.

- En este sentido son dos categorías las que definen las políticas de seguridad, estas son *Security wIPS* y *Performance Violation.* La primera categoría contempla a su vez otras que abarcan políticas para notificar ataques a nivel de protocolos así como a nivel de ataques de Denegación de Servicio y sus principales variantes. A continuación en la figura 46 se puede apreciar de mejor manera las categorías de políticas de seguridad.

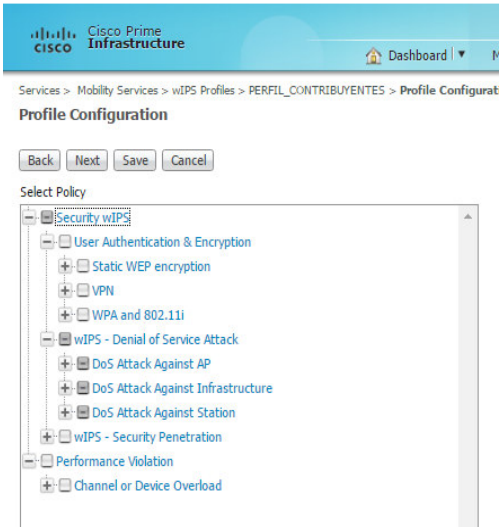


Figura 46. Categorías de seguridad predefinidas dentro de perfil wIPS creado.

Fuente: Autor.

- A pesar del número bastante amplio de políticas con las que en su totalidad cuenta un perfil wIPS creado, se ha parametrizado solo un cierto número de políticas, prioritariamente basado en los tipos de ataques más comunes documentados

anteriormente en el Marco Teórico del presente proyecto de tesis y con la ambición de apegarse a la realidad del entorno en donde la agencia principal de la "Empresa Pública de Recaudación de Impuestos" desempeña sus actividades. Además se cree son significantes para garantizar una detección temprana de los ataques más comunes a la red inalámbrica de contribuyentes. Es así que la figura 47 muestra de manera breve las políticas activadas dentro de la categoría *DoS Attack Against AP*.

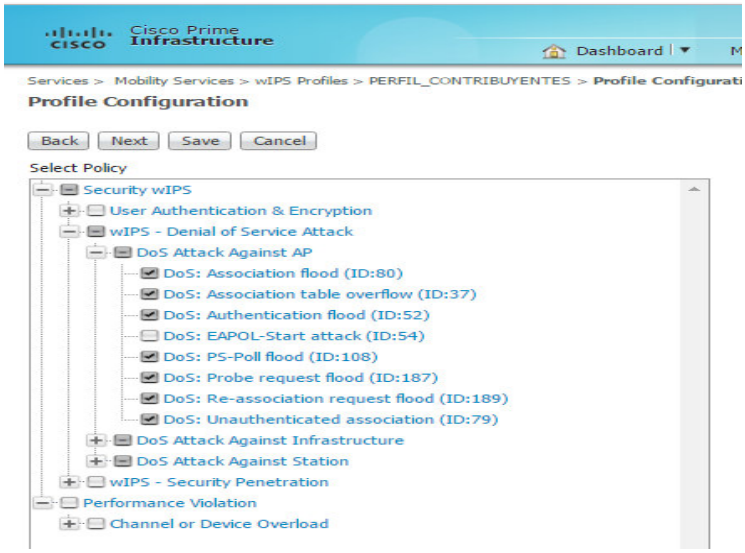


Figura 47. Categorías de seguridad DoS Attack Against AP.

Fuente: Autor.

- Los criterios utilizados para su configuración dependen de las mejores prácticas recomendadas por Cisco mediante su documentación, sin embargo la experiencia del administrador de red facilita la posibilidad de que cada alarma sea editada a futuro para obtener un análisis minucioso y obtener el resultado deseado; para efectos explicativos, se mostrará la configuración para ciertas alarmas configuradas en distintas categorías tomando en cuenta que:

- Se destaca que el criterio de Cisco respecto a la severidad del ataque indica el impacto que un ataque tiene en contra de la operación de la infraestructura.

- Por otra parte el parámetro *Número de asociaciones activas por periodo de muestreo* es equivalente a *un minuto* de tiempo acumulado en un mismo canal; es también llamado threshold o umbral y será en muchos casos diferente y dependiente del tipo de alarma.

- **DoS: Asociation Flood** .- Esta política está contemplada dentro de la categoría DoS Attack Against AP y pretende delatar la variante de un ataque DoS basado en inundar al AP con un gran número de asociaciones falsas generadas por un atacante, lo que generaría que clientes legítimos no puedan ubicarse en el estado de asociado y como resultado no podrían tener conectividad al SSID en este caso "SRI_CONTRIBUYENTES". Su configuración establece una severidad crítica tomando como buena práctica el número de asociaciones activas por minuto recomendadas y dicha política está siendo aplicada a la WLAN de contribuyentes. A continuación la figura 48 muestra lo explicado.

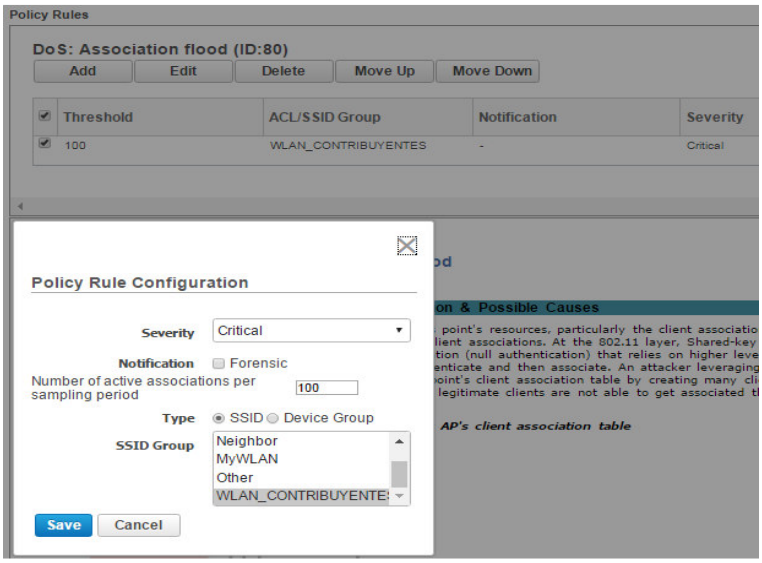


Figura 48. Configuración politica DoS Association flood.

Fuente: Autor.

- **DoS: MDK3-Destruction attack**.- Esta política está contemplada dentro de la categoría *DoS Attack Against Infrastructure* y tiene la función de alertar esta variante de un ataque DoS que ejecuta tres acciones paralelas; inunda el medio con beacons que indican la existencia de falsos AP's, ataque de inundación de autenticación y termina todas las conexiones establecidas. En este sentido la política activada se configura con una severidad Crítica a fin de que el Administrador de red sea notificado y de ser necesario capture paquetes mediante su opción *Forensic* para análisis posterior. A continuación la figura 49 muestra lo explicado.

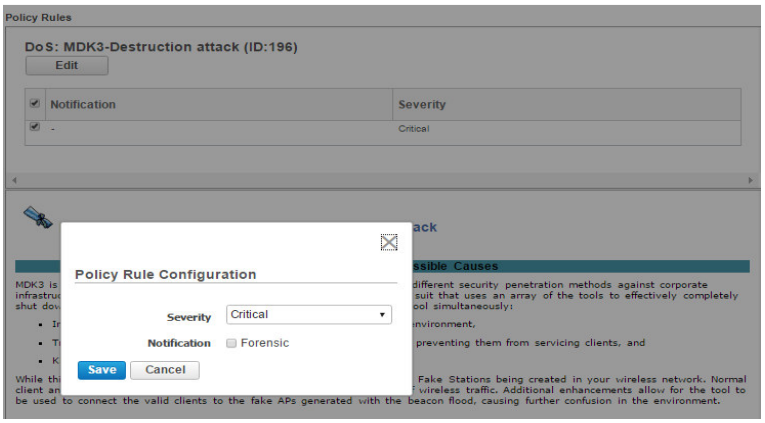


Figura 49. Configuración politica DoS MDK3-Destruction attack.

Fuente: Autor.

- **DoS: Probe response flood**.- La política *DoS: Probe response flood* está alojada dentro de la categoría *DoS Attack Against Station* y tiene por objetivo detectar cuando un atacante inunda de mensajes *Probe response* falsos que impedirían a una estación cliente poder asociarse a un AP corporativo legítimo. Para detectar este ataque, la política configurada contempla una severidad de alerta etiquetada como *Warning* complementada con un muestreo de 60 Probe Response frames por minuto, es decir si este valor es superado se notificara la presencia de un ataque de éste tipo. A continuación la figura 50 muestra lo comentado.

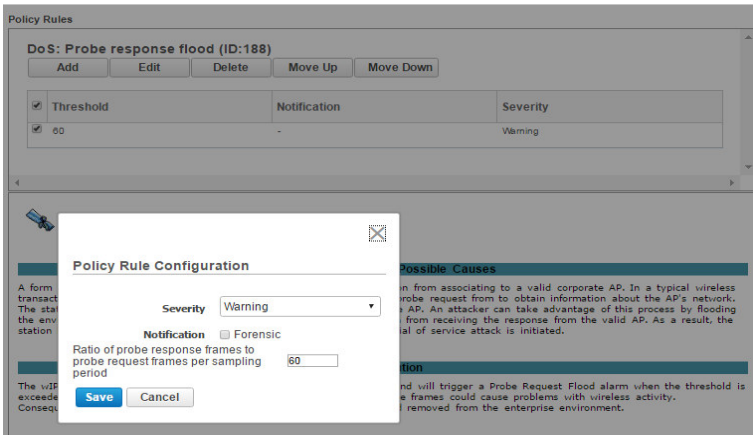


Figura 50. Configuración política DoS Probe response flood.

Recuperado: Autor.

- **Spoofed MAC address detected**.- Esta política está alojada dentro de la categoría *wIPS Security Pentration* y tiene por objetivo detectar un intento de conexión desde una AP o una estación cliente con una dirección física falsificada que ha sido modificada en su identificador organizacional o ID del fabricante mediante herramientas afines a este objetivo como smac, macchanger, etc. A continuación la figura 51 muestra la configuración de la política que contempla una severidad categorizada como *Major* y considera una muestra de 64 *Beacon Frames* tanto del *AP legítimo* así como del *AP ilegítimo.*

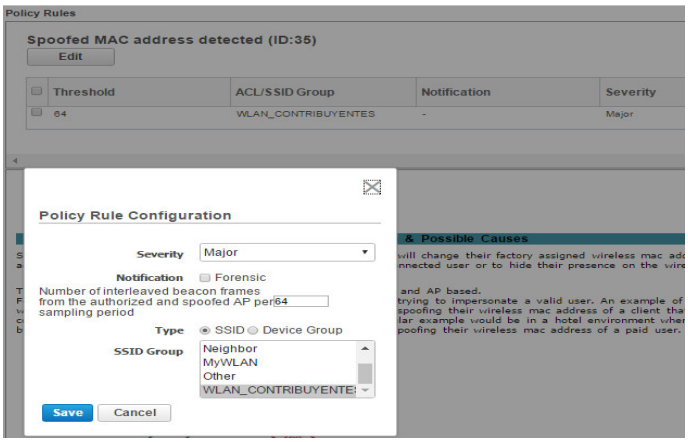


Figura 51. Configuración política Spoofed MAC address detected.

Fuente: Autor.

4 CAPÍTULO IV: PROPUESTA DE POLÍTICA BYOD PARA DISPOSITIVOS MÓVILES

En el capítulo anterior se mencionó la situación actual de la red inalámbrica interna para funcionarios así como de la red inalámbrica externa para contribuyentes, su contenido ofrecerá ciertos argumentos de sustento para el presente capítulo en donde se realiza una propuesta de política BYOD para la red interna definida para los funcionarios y que será puesta a consideración del departamento de TI de la "Empresa Pública de Recaudación de Impuestos" como un primer acercamiento en éste ámbito para futuras investigaciones, considerando que formalmente, a la fecha de la realización del presente proyecto de tesis, no existe un documento de esta naturaleza.

4.1 Propuesta de política BYOD

Es oportuno establecer , a manera de línea base, ciertos componentes con los que cuenta la "Empresa Pública de Recaudación de Impuestos" que pueden constituirse a futuro como su valor agregado para un acercamiento más formal previo a la decisión de implementar esquemas o programas BYOD.

Dichos componentes son:

- Cisco Identity Service Engine.
- Red inalámbrica para funcionarios a nivel nacional.

Con los elementos descritos en el punto 2.6.3 Políticas BYOD y tomando como punto de partida la arquitectura de política BYOD referida anteriormente en la figura 23, será planteada la política BYOD para la "Empresa Pública de Recaudación de Impuestos".

Así, la arquitectura de política propuesta a continuación contempla tres capas dentro de las cuales se desglosa mediante lineamiento, los mecanismos que garanticen un cierto nivel de gestión, control y seguridad y que pueden apreciarse de mejor manera en la figura 52.

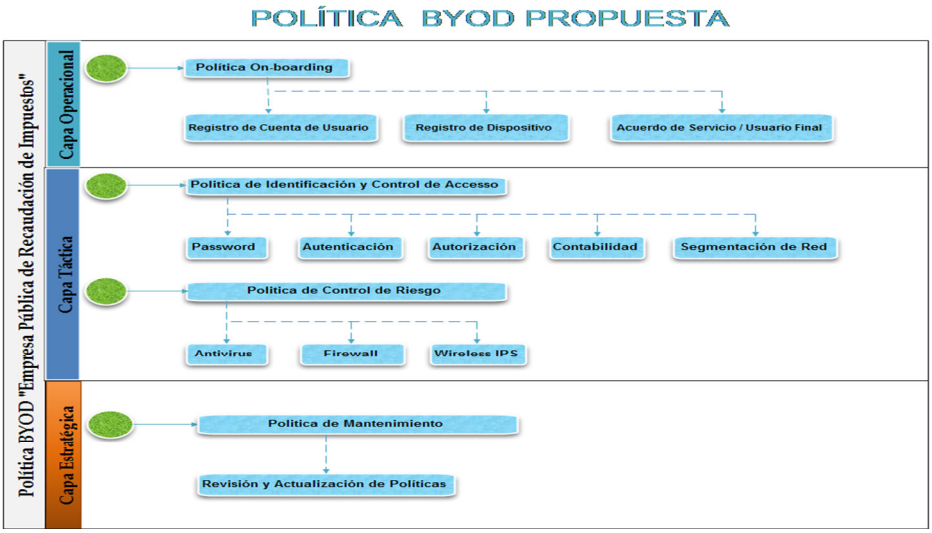


Figura 52. Arquitectura de Política BYOD propuesta.

Fuente: Autor.

4.1.1 Capa Operacional

La capa operacional es la primera capa de una arquitectura BYOD basado en políticas y trabaja conjuntamente con las políticas establecidas en las capas subsiguientes.

4.1.1.1 On-boarding Policy.

Los objetivos de la On-Board Policy o *política de abordamiento* tiene por objetivos determinar los mecanismos para que el personal de la "Empresa Pública de Recaudación de Impuestos" puedan incluir su dispositivo en el esquema BYOD, que tipo de dispositivo

está permitido así como la cantidad de dispositivos que cada funcionario podrá incluir en dicho esquema.

Así, para que un dispositivo pueda ser puesto On-Boarding es necesario que el dispositivo BYOD supere tres etapas o controles que son: registro de cuenta de usuario, registro de dispositivo y aceptación de un acuerdo de servicio para usuario final, procesos que en su conjunto deberán ser automáticos, es decir sin intervención del personal de TI.

Para que la política sea debidamente aplicada, el paso previo será la conexión a la SSID que corresponda a la red inalámbrica interna para funcionarios de la "Empresa Pública de Recaudación de Impuestos" posteriormente a lo cual deberán ser redireccionados a un portal de autoregistro en donde se ejecutarán los siguientes controles:

- **Registro de Cuenta de Usuario**.- Para usuarios nuevos será un proceso de una sola vez y consiste en proveer información que identifique al usuario como por ejemplo: un identificador de usuario, su respectiva contraseña, departamento, cargo, etc.

- **Registro de Dispositivo**.- Este proceso contempla proveer información relevante acerca de su dispositivo como por ejemplo: marca, modelo, serie, código IMEI y dirección física.

- **Acuerdo de Servicio / Usuario Final**.- Este proceso se encuentra al final de las tres etapas y contempla que el usuario final debe aceptar el acuerdo de uso del esquema BYOD en el cual se menciona un conjunto de requerimientos de índole legal respecto al uso de recursos institucionales y riesgos a los que el dispositivo BYOD de propiedad del funcionario puede estar expuesto.

4.1.2 Capa Táctica

Su función principal es la de brindar soporte en aspectos de seguridad de la información y administración de la privacidad.

4.1.2.1 Política de Control de Acceso e Identidad.

Ésta política se enfocará en establecer procedimientos y medidas de identificación y control de acceso a la información institucional en un esquema BYOD.

Los principales componentes de ésta política se describen brevemente a continuación:

- **Passwords**.- Este punto definirá las condiciones que deberán cumplir las claves de manera que se garantice reforzamiento en los mecanismos de acceso que requieran clave y se evite accesos no autorizados.

- **Autenticación**.- El control de autenticación pretende identificar que quien intenta conectarse mediante un dispositivo BYOD es quien dice ser al igual que su dispositivo, lo cual se consigue mediante usuario y contraseña y un certificado digital.

- **Autorización**.- El control de autorización define privilegios y tipos de accesos a recursos y sistemas de la empresa.

- **Contabilidad**.- El control de contabilidad refiere un mecanismo en el cual se pueda evidenciar los registros de conexiones en donde se verifique quien y que se conectó a los recursos de la empresa.

- **Segmentación de red**.- El objetivo de este control es clasificar quién y qué dispositivos pueden conectarse a que red, lo que implica que la red deba tener en el caso inalámbrico SSID's diferentes.

4.1.2.2 Política de Control de Riesgo.

La política de control de riesgo estará enfocada en proveer mecanismos de control para garantizar protección en contra de potenciales riesgos, amenazas y vulnerabilidades.

Los principales componentes que pretender brindar un esquema de seguridad a la presente política se describen brevemente a continuación:

- **Firewall**.- Este control definirá mecanismos de filtrado de tráfico hacia aquellos recursos de la empresa a los cuales un usuario o dispositivo BYOD según su rol pueden acceder. Se incluye a continuación en la tabla 9, un listado completo de puertos que deberán estar configurados o controlados en el firewall institucional a fin de contar con la comunicación monitoreada de aquellos servicios que un esquema BYOD basado en Cisco ISE y sus principales componentes demandan.

Tabla 9. Principales puertos de servicios utilizados por BYOD con Cisco ISE.

	PUERTO	TIPO	FUNCIÓN
FUNCIONES INTERNAS	22	TCP	SSH
	80	TCP	HTTP
	443	TCP	HTTPS
	9060	TCP	External Restful Services
FUNCIONES EXTERNAS	389	TCP / UDP	LDAP
	3268	TCP	LDAP
	445	TCP	SMB
	123	UDP	NTP
	53	TCP / UDP	DNS
	88	TCP / UDP	KERBEROS / KDC
	464	TCP	KERBEROS / KPASS
BYOD	8000-8999	TCP	Portal Invitados y Provisionamiento clientes.
	8443	TCP	Provisionamiento mediante asistente en S.O. Win y Mac.
	443	TCP	Provisionamiento Android mediante asistente para instalación desde Google Play.
	8905	TCP	Provisionamiento suplicante.
	9996	UDP	NetFlow
	67	UDP	DHCP
	68	UDP	DHCP SPAN
	161	UDP	SNMP QUERY
	162	UDP	SNMP TRAP
	1645, 1812	UDP	RADIUS PROXY FOR AUTHENTICATION
	1646, 1813	UDP	RADIUS PROXY FOR ACCOUNTING
	1700, 3799	UDP	RADIUS CoA
	9090	TCP	REDIRECT
	20154	UDP	SYSLOG.
	694	UDP	HEARBEAT
	0 - 65535	TCP / UDP	DETECCIÓN DE S.O. DEL ENDPOINT MEDIANTE NMAP.

Fuente: Adaptado de (Woland & Redmon, 2015)

- **Antivirus**.- Se planteará la inclusión de un mecanismo que garantice la limpieza de posible software malicioso que actué como backdoor para robo de información desde dispositivos BYOD.

- **Wips**.- Su objetivo específico será proponer la segmentación de la red inalámbrica y que se aplique el monitoreo wIPS en ella para contar con registros de posibles ataques desde dispositivos BYOD.

4.1.3 Capa Estratégica

La capa estratégica de la arquitectura propuesta, se enfocará en proponer una política de mantenimiento que contemplará la revisión de las políticas vigentes.

4.1.3.1 Política de Mantenimiento.

Bajo el esquema propuesto, dentro de la política de mantenimiento se establecerán aspectos relevantes acerca de la periodicidad de las revisiones y mejoras a realizarse en la misma con el afán de reforzar la seguridad de todos los involucrados en el esquema BYOD propuesto.

De esta manera se plantea la propuesta de política BYOD en el anexo 5 en función de la arquitectura por capas explicada en párrafos anteriores.

5 CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Como producto de la investigación realizada en el contexto de los objetivos planteados para el presente proyecto de tesis, se ha obtenido ideas y conocimientos puntuales que aportan significativamente la profesionalización de su autor así como de quien tome el presente proyecto de tesis como una fuente bibliográfica- A continuación se presentan las principales conclusiones:

- A pesar de existir distintos mecanismos de seguridad para redes 802.11, ninguno garantiza un nivel de seguridad impenetrable, sin embargo una de las mejores combinaciones para proveer un alto nivel de seguridad a una red inalámbrica en entornos corporativos es WPA2-enterprice con AES considerando que éste último maneja un mecanismo de cifrado por bloque y aleatoriza la transmisión de cada uno, lo que dificulta por mucho cualquier tipo de ataque, a pesar de ello no es concluyente asegurar que sea un mecanismo cien por ciento seguro.

- El estándar IEEE 802.11i cuenta con los mecanismos de seguridad; autenticación y encriptación, que garantizan un bajo impacto frente a posibles ataques, sin embargo con las configuraciones adecuadas al único ataque al que podría estar expuesto, así como otros mecanismos de seguridad en redes inalámbricas es al espionaje o eavesdrooping.

- Los access points brindan una visibilidad completa de la red inalámbrica y sus incidentes, sin embargo los modos de funcionamiento denominados *Local Mode* y *Flexconnect* brindan una menor efectividad que disponer de dichos Access points en modo *Monitor*; lastimosamente esto genera una desventaja que demanda disponer de un Access point para la data y otro para monitoreo que se traduce en mayor inversión económica para el entorno corporativo.

- Entre las limitaciones de la tecnología wIPS/wIDS se resalta que no detectará mecanismos de espionaje como eavesdropping por cuanto éste, realiza un escaneo pasivo del medio inalámbrico y lógicamente resulta casi imposible detectar quién olfatea el tráfico de una red "privada", por lo cual se hace imperativo reforzar la seguridad a nivel de mecanismos de autenticación, encriptación, etc.

- La "Empresa Pública de Recaudación de Impuestos" cuenta con la infraestructura necesaria para implementar un esquema BYOD basado en su principal componente de políticas de seguridad Cisco ISE; de manera que se concluye que es factible la incorporación de iniciativas que a futuro faciliten la decisión de adoptar dicho esquema.

- Para la implementación de un esquema BYOD que garantice principalmente seguridad, confidencialidad, control de dispositivos y sus respectivos accesos es concluyente la necesidad de contar con sistema MDM.

5.2 RECOMENDACIONES

A continuación se presentan las recomendaciones que tiene por objetivo la mejora de aquellos aspectos relacionados con las líneas de investigación del presente proyecto de tesis y que a su vez buscan el beneficio de la institución.

- Con el afán de mejorar la seguridad en otras aristas que en el presente proyecto de tesis pudieron no mencionarse, se recomienda configurar la opción *Rogues* en el WLC con el fin de incluir las direcciones físicas o mac address de aquellos dispositivos que pueda comprobarse que no son generadores de trafico anómalo lo cual permitiría sesgar el número de dispositivos que puedan ser monitoreados y disponer así de una visión más concreta de los dispositivos ajenos a la institución.

- En pro de mantener las plataformas al día se recomienda actualizar LAS plataformas que manejan los puntos críticos de la infraestructura inalámbrica que para el presente caso de estudio son el Wireless Lan Controller así como Cisco Prime Infrastructure y Cisco Mobility Services Engine a sus versiones estables más recientes.

- La optimización del espacio de almacenamiento de Cisco PI es recomendable por cuanto las configuraciones de alarmas y políticas wIPS que tienen activado el parámetro forense generarán gran cantidad de log's o registros de eventos lo que ocupará gran espacio considerable con el tiempo.

- Con el afán de realizar un análisis profundo sobre los posibles ataques que no se contemplen en la configuración propuesta, se recomienda modificar cada política wIPS generada para cada alarma y se incluya el parámetro "forense" con el afán de que cada AP genere un archivo *.CAP que contenga los datos recuperados de una muestra obtenida del entorno inalámbrico, sin embargo el proceso de generación de dicho archivo puede aumentar dramáticamente el tráfico generado por las alarmas. Es recomendable activar dicha opción con criterio para casos específicos en donde se requiera un análisis minucioso de eventos críticos.

- En beneficio de la institución es recomendable que se incluyan perfiles de análisis y monitoreo wIPS adicionales y que éstos contemplen otros niveles de severidad en sus reglas de política, lo que permitirá tener un monitoreo más detallado en contra de posibles ataques.

- Con el interés de garantizar la seguridad a nivel de la red inalámbrica orientada a funcionarios y evitar posibles ataques internos, es recomendable que se planifique la implementación de módulos WSM a nivel nacional y de manera estratégica ubicarlos en aquellos espacios que demanden alto flujo de datos. Esta recomendación se la realiza en apego a los procesos y gestiones internas institucionales previas a una adquisición.

- Es altamente recomendable que se realicen las pruebas, estudios y demás análisis que evalúen la posibilidad de incorporación de un sistema MDM para justificar una futura adopción de un esquema BYOD a nivel de la "Empresa Pública de Recaudación de Impuestos" que tendrá por objetivo principal una reducción de costos en el aprovisionamiento de equipos para el segmento de funcionarios

móviles y por otra parte proveerá una administración centralizada de aquellos dispositivos de propiedad del empleado.

6 BIBLIOGRAFÍA

Academia Cotopaxi. (s.f.). *Bring Your Own Device [BYOD].* Obtenido de https://www.cotopaxi.k12.ec/BYOD

Alonzo, M. (15 de 05 de 2013). *BYOD: Ventajas, desventajas y consideraciones de Seguridad.* Obtenido de TIB Seguridad en la Información : http://tib.com.uy/blog/

Asamblea Nacional del Ecuador. (2014). Código Orgánico Integral Penal. *Registro Oficial*, 36-37.

Assee, D. (02 de 06 de 2011). *SlidePlayer.* Obtenido de Billing Operations and Information Technology (Focus in IT Security Rules): http://slideplayer.com/slide/3547052/

Balseca Guzmán, L. A. (21 de 06 de 2013). Estado de arte en la detección de intrusiones en redes 802.11. Quito, Pichincha, Ecuador.

Bartz, R. (2009). *Certified Wireless Technology Specialist Official Study Guide [CWTS].* Indianapolis: Wiley.

Bello, A., Armarego, J., & Murray, D. (Marzo - Abril de 2015). A Policy-Based Framework for Managing Information Security and Privacy Risks in BYOD Environments. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 4*(2), 189-198.

Boyle, R. J., & Panko, R. R. (2013). *Corporate Computer Security Third Edition* (Third ed.). New Jersey: Pearson.

Brooks, R. (2014). *Introduction to computer and network security.* Boca Raton, FL: CRC Press.

Cavoukian, A. (12 de 2013). *Information and Privacy Commissioner of Ontario.* Obtenido de BYOD (Bring your Own Device) Is your Organization Ready?: https://www.ipc.on.ca/wp-content/uploads/2013/12/pbd-byod.pdf

Chandra, P., Bensky, A., Bradley, T., Hurley, C. R., Rittinghouse, J., & otros, y. (2009). *Wireless Security.* Burlington: Elsevier.

Chandramouli, V. (2002). A Detailed Study on Wireless LAN Technologies. Texas, Arlingtong, USA.

Chen , G., Yao , H., & Wang , Z. (31 de 12 de 2009). *IEEE Xplore Digital Library.* Obtenido de Research of wireless intrusion prevention systems based on plan recognition and honeypot: http://ieeexplore.ieee.org/document/5371448/?arnumber=5371448&newsearch=true&queryText=Wireless%20intrusion%20prevention%20system

Chen, L., Jiahuang, J., & Zihong, Z. (Edits.). (2013). *Wireless Network Security: Theories and Applications.* New York: Springer-Verlag Berlin Heidelberg.

Cheswick, W., Bellovin, S., & Rubin, A. (2003). *Firewalls and Internet security: repelling the wily hacker.* Massachusetts: Addison-Wesley Longman Publishing.

Ciampa, M. (2013). *Guide to Wireless LANs [CWNA]* (3rd. ed.). Boston: Cengage Learning.

CISCO. (2014). *Cisco Wireless Intrusion Prevention System Data Sheet*. Obtenido de Cisco Wireless Intrusion Prevention System Data Sheet: http://www.cisco.com/c/en/us/products/collateral/wireless/adaptive-wireless-ips-software/data_sheet_c78-501388.html

CISCO. (s.f.). *Cisco Aironet Access Point Module for Wireless Security Data Sheet [WSSI]*. Recuperado el 27 de 01 de 2017, de Cisco Aironet 3700 series: http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps11983/data_sheet_c78-720719_ps13367_Products_Data_Sheet.html

Coleman, D., & Westcott, D. (2006). *Certified Wireless Network Administrator Guide [CWNA].* Indianapolis: Wiley.

Coleman, D., Westcott, D., Harkins, B., & Jackman, S. (2010). *CWSP Certified Wireless Security Professional Official Study Guide.* Indianapolis: Wiley.

Columbus Luis. (12 de 09 de 2013). *FORBES*. Obtenido de IDC: 87% Of Connected Devices Sales By 2017 Will Be Tablets And Smartphones: http://www.forbes.com/sites/louiscolumbus/2013/09/12/idc-87-of-connected-devices-by-2017-will-be-tablets-and-smartphones/#341880b22472

De Paz, S. (2010). *Estudio de vulnerabilidad de los cifrados WEP y WPA, y su impacto en las Redes Inalámbricas de área local. (Tesis de Pregrado).* Guatemala: Universidad de San Carlos de Guatemala.

Delitos Informaticos. (2015). *Delitos Informaticos*. Obtenido de División Computer Forensic: http://www.delitosinformaticos.info/peritaje_informatico/estadisticas.html

Dewdney, A. (Marzo de 1989). Computer Recreations: Of Worms, Viruses and Core War. *Scientific American*, 110.

Diogenes, Y., & Gilbert, J. (2015). *Enterprise Mobility Suite Managing BYOD and Company-Owned Devices.* Washington: Microsoft Press.

Earle, A. (2006). *Wireless Security Handbook.* New York: Taylor&Francis Group.

ESET. (2012). *INFORC ECUADOR*. Obtenido de BYOD: Infografía sobre los nuevos desafíos para las empresas: http://www.inforc.ec/category/byod/

Giusto Bilić, D. (07 de 01 de 2016). *WELIVESECURITY.* Obtenido de ¿Qué son las soluciones MDM y por qué debes tenerlas en mente?: http://www.welivesecurity.com/la-es/2016/01/07/que-son-las-soluciones-mdm/

González, D. (2003). *Sistemas de Detección de Intrusiones.* Obtenido de https://www.dgonzalez.net/: https://www.dgonzalez.net/papers/ids/IDS_v1.0.pdf

Granja, C., & Vallejo, R. (2015). *Adopción de un Marco Metodológico de Arquitectura Empresariall en una empresa gubernamental, Caso de estudio Administración de Impuestos (Tesis de maestría).* Quito: Pontificia Universidad Católica del Ecuador.

Graves, K. (2007). *CEH Official Certified Ethical Hacker.* Indianapolis: Wiley Publishing.

Guaño Aucancela, M. S., & Novillo Ortega, C. P. (26 de 03 de 2012). Implementación de un sistema de detección de intrusos utilizando inteligencia artificial. Quito, Pichincha, Ecuador.

Guttman, B., & Roback, E. (1995). *An introduction to Computer Security: The NIST Handbook.*

Holt, A., & Huang, C. (2010). *802.11 Wireless Network Security and Analisis.* Dordrecht: Springer.

HP. (2010). *HP.* Obtenido de HP AirProtect Wireless Security Series: https://www.hpe.com/h20195/v2/GetPDF.aspx/c04284857.pdf

Jacobs, S. (2014). *Security management of next generation telecomunications, networks and services.* Hoboken: IEEE Press Wiley.

Khan Pathan, A.-S. (Ed.). (2014). *The State of the Art in Intrusion, Prevention and Detection.* Boca Raton: CRC Press.

Lawson, C., Hils, A., & Neiva, C. (16 de 11 de 2015). *Magic Quadrant for Intrusion Prevention Systems*. Obtenido de https://www.gartner.com/doc/3168221/magic-quadrant-intrusion-prevention-systems

López, A. (2015). *Adsmovil - Mobile Advertising Solutions.* Obtenido de La penetración de smartphones crece en América Latina.: http://www.adsmovil.com/la-penetracion-de-smartphones-crece-en-america-latina/

Maxim, M., & Pollino, D. (2002). *Wireless Security.* Osborne: McGraw-Hill.

Melero, N. (2014). *Estudio sobre la implantacipon de las políticas BYOD para el uso de dispositivos móviles personales en las comunicaciones de empresa (Tesis de Pregrado).* Valencia: Universidad Politécnica de Valencia.

MICROSOFT. (19 de Abril de 2011). *Consumerización de la TI: Preguntas más frequentes*. Recuperado el 28 de Enero de 2017, de Centro de TI de Windows: https://technet.microsoft.com/es-es/windows/hh182564.aspx

MICROSOFT CORPORATION. (2017). *Microsoft Tech*. Obtenido de Diseño de un servidor de seguridad perimetral: https://www.microsoft.com/spain/technet/recursos/articulos/secmod156.mspx

Migga, J. (2005). *Computer Network Security.* Chattanooga: Springer.

Migga, J. (2009). *Guide to security network.* Madrid: McGrawHill.

Migga, J. (2015). *Guide to Computer Network Security* (Third ed.). (A. Sammes, Ed.) Chattanooga: Springer.

MOTOROLA. (2011). *Motorola Wireless Intrusion Prevention Solutions Overview.* Obtenido de Solution Paper: http://www.p4it.de/frontend/media/files/airdefense_intrusion_prevention_solutions.pdf

Nagenthiran , N., Jayasekara, R., & Jayasekara, S. (2010). *Intrusion Detection & Intrusion Prevention Systems.* Obtenido de https://pdfs.semanticscholar.org/d112/09a79f3b6aa08241a3d3d141b2a3ef631021.pdf.

Northcutt, S., Zeltser, L., Winters, S., Kent, K., & Ritchey, R. (2005). *Inside Network Perimeter Security.* Indianapolis: Sams Publishing.

Oriyano, S. (2016). *CEHv9 Certified Ethical Hacker Version 9: Study Guide.* Indianapolis: Wiley.

Rhodes Ousley, M. (2013). *Information Security: The Complete Reference* (2nd. ed.). New York: McGraw-Hill.

Rob MacDonald, Rebecca Golden. (23 de 06 de 2016). *SlideShare.* Obtenido de ForgeRock Gartner 2016 Security & Risk Management Summit : http://www.slideshare.net/ForgeRock/forgerock-gartner-2016-security-risk-management-summit

RUCKUS. (2016). *Secure Onboarding.* Recuperado el 01 de 02 de 2017, de https://www.ruckuswireless.com/solutions/secure-onboarding

Sánchez Gómez, M. (06 de Julio de 2011). *https://manuelsanchez.com/*. Obtenido de https://manuelsanchez.com/2011/07/06/infraestructuras-criticas-y-ciberseguridad/

Sánchez Prieto, L. M. (24 de 05 de 2012). Diseño de un sistema de seguridad informática para la red LAN de telecomunicaciones del Ministerio de Minas y Petróleos. Quito, Pichincha, Ecuador.

Sánchez, A., & Martínez, G. (2008). IDS and IPS Systems in Wireless Communication Scenarios. En M. Khosrow, *Encyclopedia of Information Science and Technology* (Segunda ed., págs. 1799-1804). Hersey: IGI Global.

Sánchez, M. (06 de Julio de 2011). *https://manuelsanchez.com/ [Blog]*. Obtenido de Infraestructuras Críticas y Ciberseguridad: https://manuelsanchez.com/2011/07/06/infraestructuras-criticas-y-ciberseguridad/

Servicio de Rentas Internas [SRI]. (23 de Octubre de 2016). *¿Qué es el SRI?* Obtenido de http://www.sri.gob.ec/web/guest/que-es-el-sri;jsessionid=hZVBweSsqFzUD5KoSZ+yfYW+

Servicio de Rentas Internas. (8 de Mayo de 2014). Recuperado el 16 de Julio de 2015, de https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB0QFjAAahUKEwiO0eChysjIAhUDlQ0KHfpFCFI&url=http%3A%2F%2Fwww.sri.gob.ec%2FDocumentosAlfrescoPortlet%2Fdescargar%2F9e166e8c-726e-4313-b88d-c20f749f8a51%2FRESOLUCION%2BORGAN

Skrobanek, P. (Ed.). (22 de Marzo de 2011). *Intrusion Detection System and Artificial Intelligent.* Obtenido de InTech: http://www.intechopen.com/books/intrusion-detection-systems/intrusion-detection-system-and-artificial-intelligent

Stallings, W. (2011). *Network Security Essentials: Applications and standars.* Pearson.

Strebe, M. (2004). *Network Security Foundations: Technology Fundamentals for IT Success.* California: Sybex.

Stretch, J. (2016). *packetlife.net.* Obtenido de IEEE 802.11 WLAN . Part 1: http://packetlife.net/media/library/4/IEEE_802.11_WLAN.pdf

Timofte, J. (2008). Wireless Intrusion Prevention Systems. *Informática Económica, XII*, 129.

Tipton, H., & Krause, M. (Edits.). (2004). *Information Security Management Handbook.* Florida: CRC Press.

Vanjale , S. B., & Mane , P. B. (04 de 05 de 2015). *IEEE Xplore Digital Librry.* Obtenido de Wireless LAN Intrusion Detection and Prevention system for Malicious Access Point : http://ieeexplore.ieee.org/document/7100297/authors

Wikipedia. (22 de 03 de 2015). *Política de seguridad*. Recuperado el 01 de 02 de 2017, de https://es.wikipedia.org/wiki/Pol%C3%ADtica_de_seguridad

Wikipedia. (2016). Obtenido de Bring your Own Device: https://es.wikipedia.org/wiki/Bring_your_own_device.

William, S. (2011). *Network Security Essentials Application and Standards 4th Edition.* USA: Pearson.

Woland, A., & Heary, J. (2013). *Cisco ISE for BYOD and Secure Unified Access.* Indianapolis: Cisco Press.

Woland, A., & Redmon, K. (2015). *CCNP Security SISAS 300-328 Official Cert Guide.* Indianapolis, USA: Cisco Press.

Zhang , Y., Chen , G., Wang , Z., & Weng , W. (30 de 09 de 2010). *IEEE Xplore Digital Library.* Obtenido de An overview of wireless intrusion prevention systems : http://ieeexplore.ieee.org/document/5588671/

7 ANEXOS

Anexo 1: Cisco Mobility Services Engine Overview Data Sheet

Feature	Benefits
Services	**Base Location license** Track and locate Wi-Fi devices, interferers, rogues, and RFID tags Detect presence and receive geo-fenced or zone-based alerts Show system wide interferer details and correlation Visualize interferer zone of impact Develop custom applications to engage users with open location API Heighten customer experience by integrating indoor navigation experiences into loyalty apps Increase app usage by automatically connecting to the Wi-Fi network and launching loyalty apps upon arrival Discover and stop security penetration and DoS attacks Connected Mobile Experiences (CMX) license Provide simple guest access to end-users with a location-aware captive portal Manage visitors and increase brand presence with Facebook Analyze onsite customer behavior and make informed business decisions Develop custom applications to engage users with the CMX SDK wIPS license Monitor, mitigate and report security threats to the wireless network Enhance security and regulatory compliance features of WLAN with location intelligence
Platform	Physical appliance -3365 Physical appliance - 3355* Virtual appliance
Location technologies	Signal strength triangulation: Determines the location of a Wi-Fi device by triangulating the relative signal strength detected by the access points in the WLAN network. This method determines the location only of probing signals emanating from the client Wi-Fi device. FastLocate: Determines the location of a Wi-Fi device by triangulating the relative signal strength detected by the access points in the WLAN network. This method determines the location of probing signals as well as data packets emanating from the client Wi-Fi device. This increases the update rates of location calculations for devices that are connected to the WLAN network. FastLocate requires a Wireless Security Module (WSM) in every access point that takes part in the location calculation Presence: Determines the location of a Wi-Fi device by gauging the nearest access point to that device. This method provides less granular location accuracy than triangulation; however, it can be deployed in venues with fewer access points. Presence can currently be used only

Feature	Benefits
	with CMX Analytics or integrated into third-party applications using the northbound notification API.

Anexo 2: Cisco Identity Services Engine Data Sheet

Features and Benefits

Feature	Benefit
Centralized management	‣ Helps administrators centrally configure and manage profiler, posture, guest, authentication, and authorization services in a single web-based GUI console. ‣ Simplifies administration by providing integrated management services from a single pane of glass.
Business-policy enforcement	‣ Provides a rule-based, attribute-driven policy model for flexible and business-relevant access control policies. Also provides the ability to create fine-grained policies by pulling attributes from predefined dictionaries. ‣ Includes attributes such as user and endpoint identity, posture validation, authentication protocols, profiling identity, and other external attribute sources. These can be created dynamically and saved for later use. ‣ Integrates with multiple external identity repositories such as Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), RADIUS, RSA one-time password (OTP), certificate authorities for both authentication and authorization, and supports Open Database Connectivity (ODBC).
Access control	‣ Provides a range of access control options, including downloadable access control lists (dACLs), VLAN assignments, URL redirections, named ACLs, and security group tag (SGT) using the advanced capabilities of network devices enabled with Cisco TrustSec technology.
Secure supplicant-less network access with Easy Connect	‣ Provides the ability to swiftly roll out highly secure network access without configuring endpoints for authentication and authorization. ‣ Derives authentication and authorization from login information across application layers, allowing user access without requiring an 802.1X supplicant to exist on the endpoint.
Guest lifecycle management	‣ Provides a streamlined experience for implementing and customizing guest network access. ‣ Creates corporate-branded guest experiences, with advertisements and promotions, in minutes. Support is built in for hotspot, sponsored, self-service, and numerous other access workflows. ‣ Provides the administration with real-time visual flows that bring the effects of the guest flow design to life. ‣ Tracks access across your network for security and compliance demands and full guest auditing. Time limits, account

Feature	Benefit
	expirations, and SMS verification offer additional security controls.
Streamlined device onboarding	‣ Automatic supplicant provisioning and certificate enrollment for standard PC and mobile computing platforms. Reduces IT help desk cases along with providing more secure access and a better experience to users. ‣ Enables end users to add and manage their devices with self-service portals and supports SAML 2.0 for web portals. ‣ Integrates with MDM/EMM vendors to enroll mobile devices and help ensure that they are compliant with access policy.
Built-in AAA services	‣ Uses standard RADIUS protocol for authentication, authorization, and accounting (AAA). ‣ Supports a wide range of authentication protocols, including, but not limited to PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunneling (FAST), EAP-Transport Layer Security (TLS), and EAP-Tunneled Transport Layer Security (TTLS).Note: Cisco ISE is the only RADIUS server to support EAP chaining of machine and user credentials.
Device administration access control and auditing	‣ Supports TACACS+ protocol to authenticate, authorize, and audit users when they access devices that support the TACACS+ protocol, such as network devices and servers. ‣ Grants users access to commands on every device based on their credentials, the group they belong to, where they connect from, and what action they are trying to take on the device. ‣ Provides access to device configuration on a need-to-know and need-to-act basis while keeping audit trails for every change in the network.
Internal certificate authority	‣ Offers an easy-to-deploy internal certificate authority to simplify certificate management for devices. There is no need to add the significant complexity of an external certificate authority application. ‣ Provides a single console to manage endpoints and their certificates. Certificate status is checked through the standards-based Online Certificate Status Protocol (OCSP). Certificate revocation is automatic. ‣ Supports standalone deployments, products integrated on pxGrid, and subordinate ones (that is, ones in which the certificate authority is integrated with your existing enterprise public key infrastructure, or PKI). ‣ Facilitates the manual creation of bulk or single certificates and key pairs to connect these devices to the network with a high degree of security.
Device profiling	‣ Ships with predefined device templates for many types of endpoints, such as IP phones, printers, IP cameras, smartphones,

Feature	Benefit
	tablets, and over 250 medical devices. › Creates custom device templates to automatically detect, classify, and associate administration-defined identities when endpoints connect to the network. › Helps to associate endpoint-specific authorization policies based on device type. › Collects endpoint attribute data with passive network monitoring and telemetry. It queries the actual endpoints or, alternatively, the Cisco infrastructure using device sensors on Cisco Catalyst® switches.
Device-profile feed service	› Delivers automatic updates of Cisco's validated device profiles for various IP-enabled devices from multiple vendors. It detects all the newest devices and simplifies the task of keeping up with them. › Partners and customers can share customized profile information to be vetted by Cisco and redistributed.
Endpoint posture service	› Performs endpoint posture assessment on PCs and mobile devices connecting to the network. › Works through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM vendors system to validate that an endpoint conforms to appropriate compliance policies. › Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patches, antivirus and antispyware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock or rooted or jailbroken status, application presence, USB attached media and so on. › Supports the automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies. › Requires the AnyConnect 4.x agent for posture assessment on these OS platforms: Microsoft Windows 7, 8, or 10 (32-bit or 64-bit) and Mac OS X 10.7, 10.8, 10.9, or 10.11.
Extensive multi-forest Active Directory support	› Provides comprehensive authentication and authorization against multi-forest Microsoft Active Directory domains. › Groups multiple disjointed domains into logical groups. Configurations of complex Active Directory topologies are simplified to support ever-changing business environments. › Includes flexible identity rewriting rules to smooth the solution's transition and integration. › Supports Microsoft Active Directory 2003, 2008, 2008R2, 2012, and 2012R2.
Cisco Rapid Threat	› Takes manual or automated network mitigation and

Feature	Benefit
Containment	investigation actions in response to security events. • Integrates Cisco ISE and Cisco security technology partner solutions in a broad variety of technology areas. • Changes user access based on CVSS vulnerability and STIX threat scores. • Uses Cisco pxGrid as a highly scalable IT clearinghouse for multiple security tools to communicate with each other in real time, automatically.
Monitoring and troubleshooting	• Offers a built-in web console for monitoring, reporting, and troubleshooting to assist help desk and network operators in quickly identifying and resolving issues, including Cisco Security Technology Alliance partners. • Provides robust historical and real-time reporting for all services. Logs all activities and offers real-time dashboard metrics of all users and endpoints connecting to the network.
Certifications	• Meets the requirements of Federal Information Processing Standard (FIPS) 140-2, Common Criteria, and Unified Capabilities Approved Product List. Also IPv6 ready. • Note: Certifications may not be available on all releases, or they may be in varying states of approval. Current certifications and releases can be found atGlobal Government Certifications.

Anexo 3: Configuración Access Points con módulo WSM.

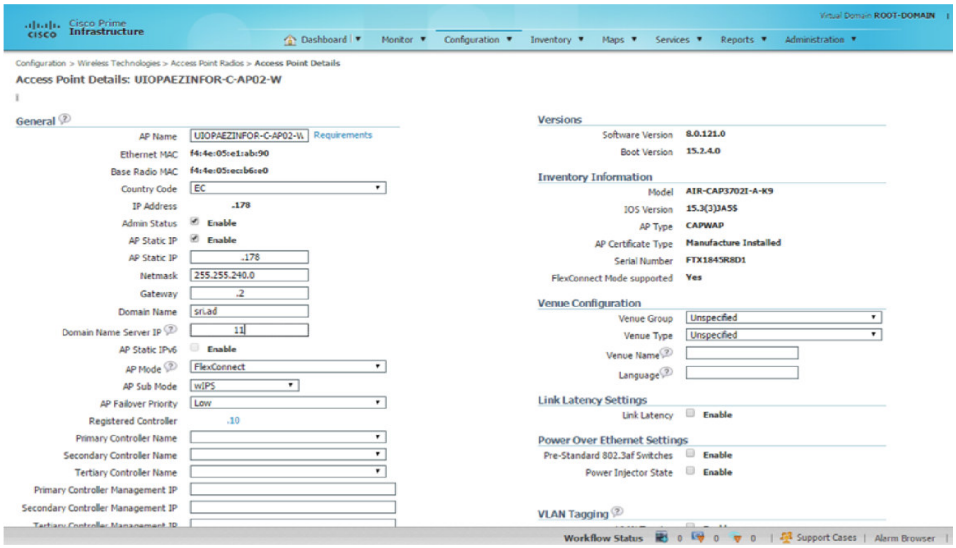
En base a la tabla 8, presentada en el capítulo 3, ítem 3.2.2.2 WIPS en la "Empresa Pública de Recaudación de Impuestos", a continuación se presenta de manera gráfica la configuración planteada para los tres acces points que cuentan con un módulo WSM.

La metodología con la que se procedió en cada AP fue la siguiente:

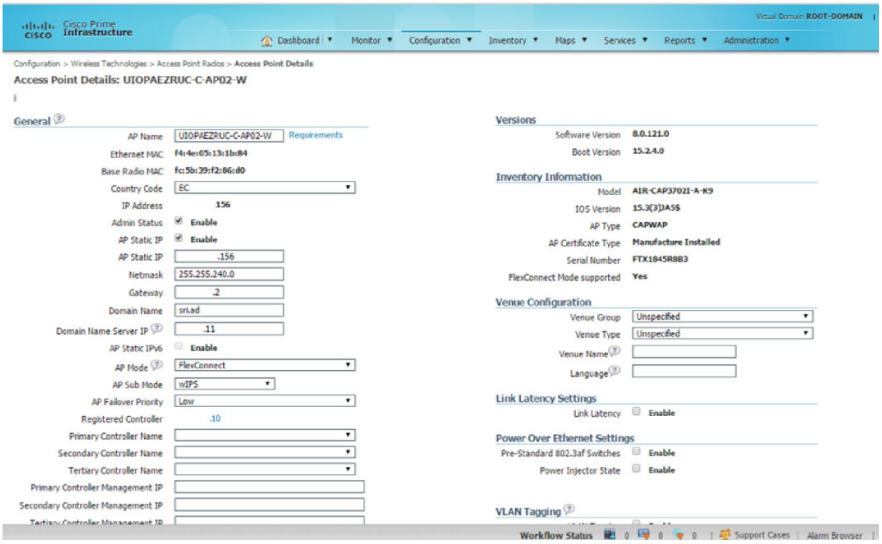
- Deshabilitar *Admin Status*.
- Habilitar modo FlexConnect.
- Habilitar compatibilidad con wIPS.
- Habilitar *Admin Status*.
- Reiniciar AP.

Como se mencionó en el ítem 3.3.2 Configuración propuesta para Access Points, la configuración puede ser realizada desde el WLC así como desde Cisco Prime Infrastructure. Así la configuración para cada AP se la implementó desde Cisco Prime Infrastructure de la siguiente manera.

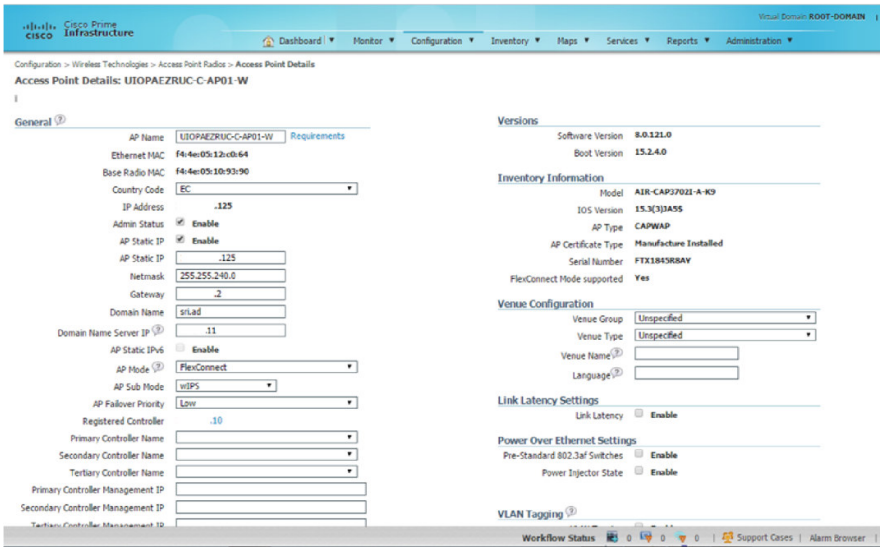
Access Point: UIOPAEZINFOR-C-AP02-W



Access Point: UIOPAEZRUC-C-AP02-W



Access Point: UIOPAEZRUC-C-AP01-W



Anexo 4: Configuración Cisco MSE – Cisco Prime Infrastructure

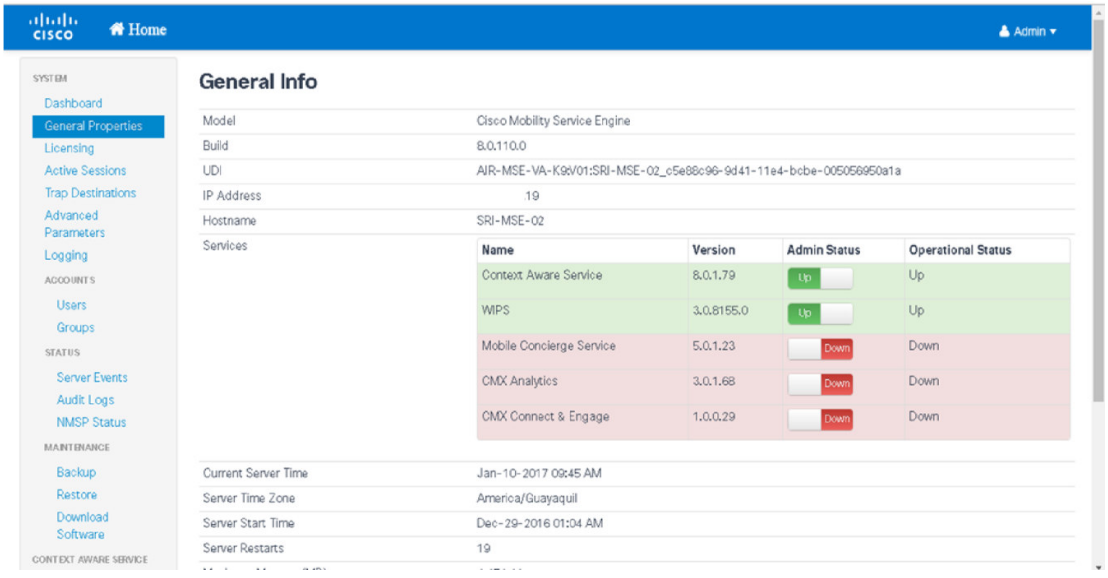
La metodología adoptada para la configuración de los perfiles WIPS en la plataforma Cisco MSE ha sido la detallada en el ítem 3.3.3 Configuración propuesta para Cisco MSE – Cisco Prime Infrastructure del capítulo III.

Lor procedimientos utilizados se detallan a continuación:

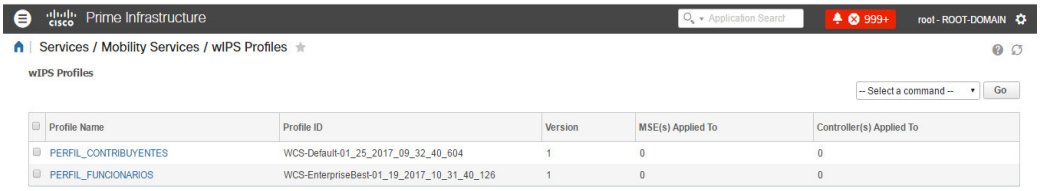
- Creación de dos perfiles WIPS que permita diferenciar el o los SSID's a los que se aplique el monitoreo.
- Creación de un Grupo de SSID denominado WLAN_CONTRIBUYENTES.
- Configuración de políticas y alarmas de seguridad WIPS.
- Aplicación de perfiles WIPS a WLC y AP's.

En este sentido, a continuación se muestra de manera gráfica las configuraciones implementadas.

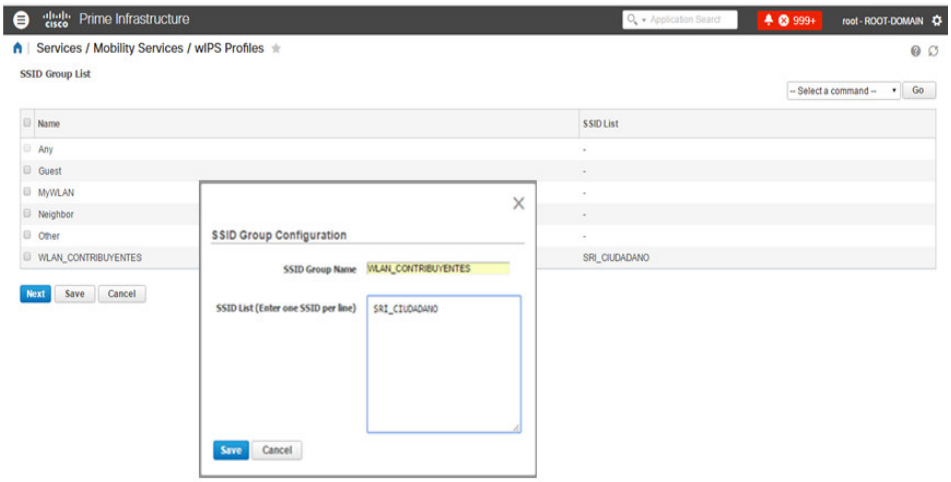
a) Licenciamiento.- Se ha validado que el licenciamiento esté vigente y activo dentro de la plataforma MSE-02, procedimiento que habilita el monitoreo mediante la tecnología WIPS.



b) Se crearon dos perfiles WIPS denominados “PERFIL_CONTRIBUYENTES” y “PERFIL_FUNCIONARIOS”, con el objetivo de diferenciar la aplicación de monitoreo WIPS por SSID.



c) El perfil sobre el cual se configurará las políticas de seguridad y alarmas WIPS será “PERFIL_CONTRIBUYENTES” fundamentado en la situación actual en donde se estipula que en la agencia principal de la “Empresa Pública de Recaudación de Impuestos” se cuenta con tres AP’s con módulo WSM y adicionalmente cuenta con aproximadamente 48 AP’s con dicho módulo distribuidos a nivel nacional.



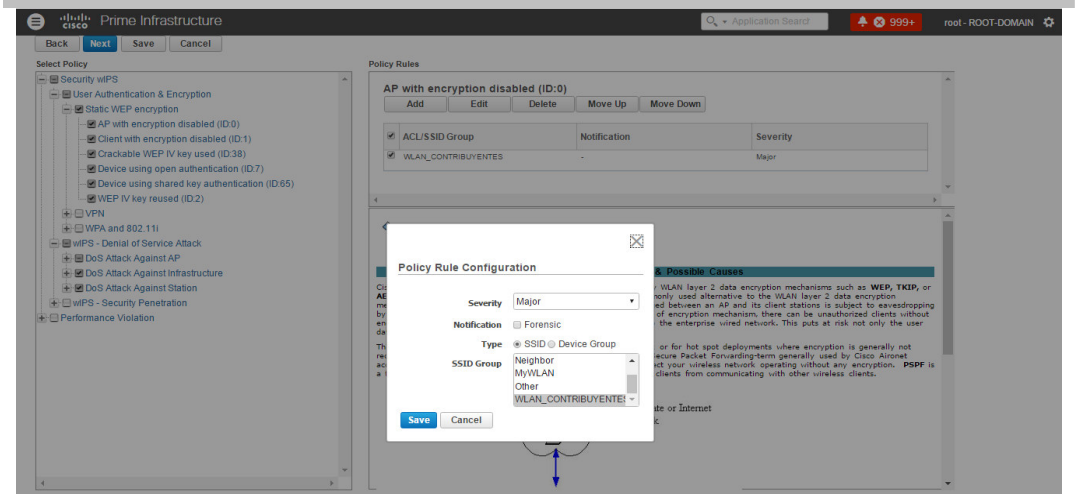
d) La siguiente etapa de la implementación contempla la configuración de ciertas políticas de seguridad y alarmas contenidas en la categoría *Security Wips*.

CATEGORIA: SECURITY WIPS

SUBCATEGORIA: USER AUTHENTICATION & ENCRYPTION

POLÍTICA: STATIC WEP ENCRYPTION

ALARMA: AP WITH ENCRYPTION DISABLED

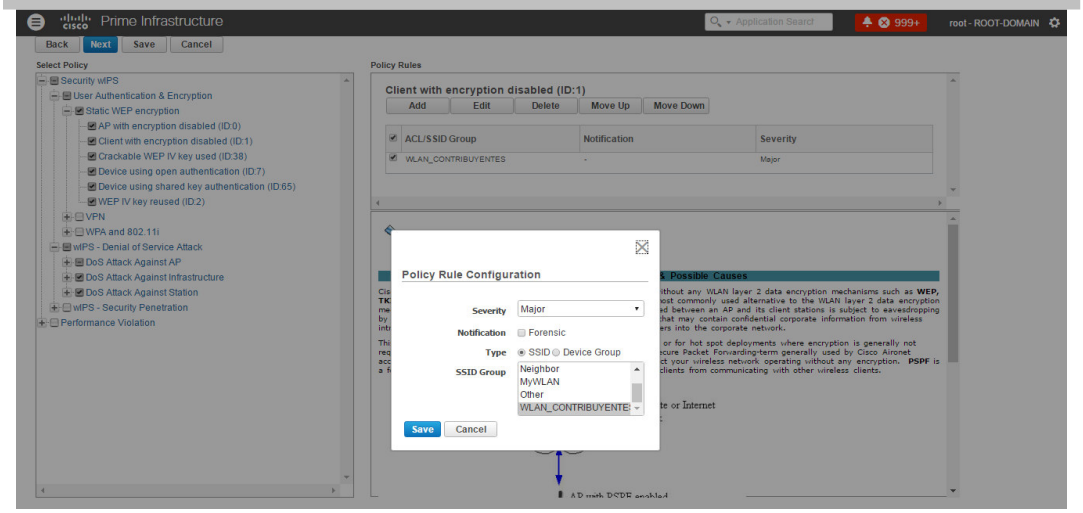


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: USER AUTHENTICATION & ENCRYPTION

POLÍTICA: STATIC WEP ENCRYPTION

ALARMA: CLIENT WITH ENCRYPTION DISABLED

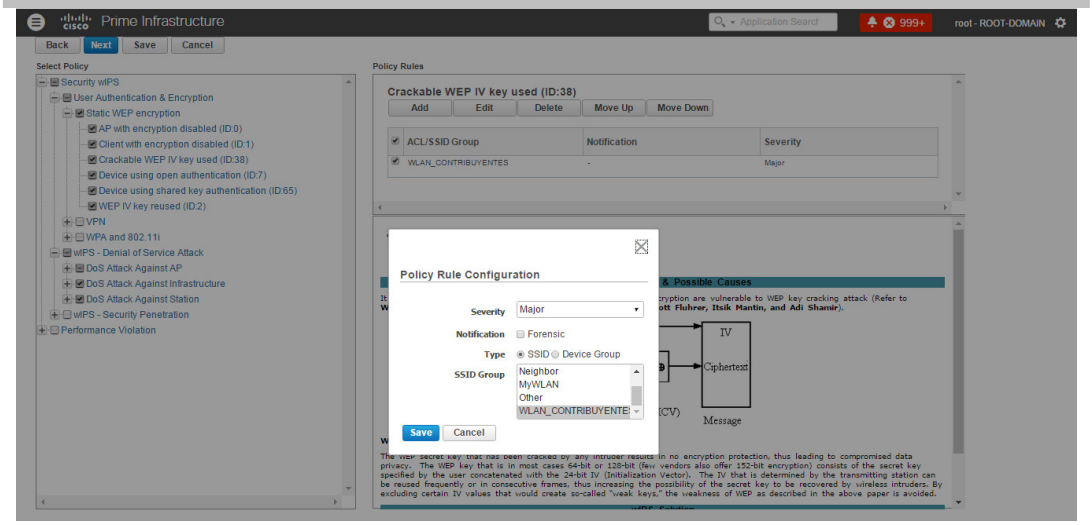


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: USER AUTHENTICATION & ENCRYPTION

POLÍTICA: STATIC WEP ENCRYPTION

ALARMA: CRACKABLE WEP IV KEY USED

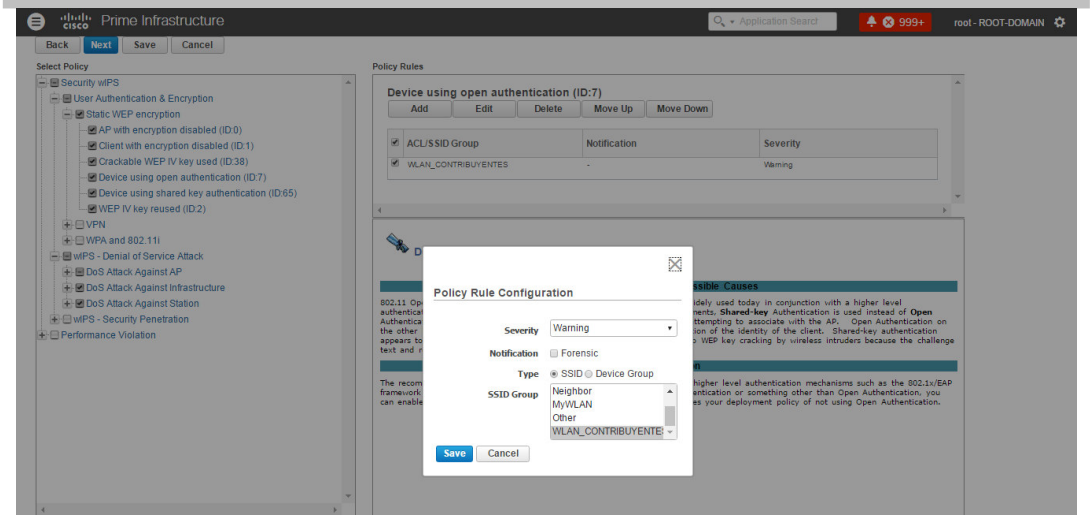


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: USER AUTHENTICATION & ENCRYPTION

POLÍTICA: STATIC WEP ENCRYPTION

ALARMA: DEVICE USING OPEN AUTHENTICATION

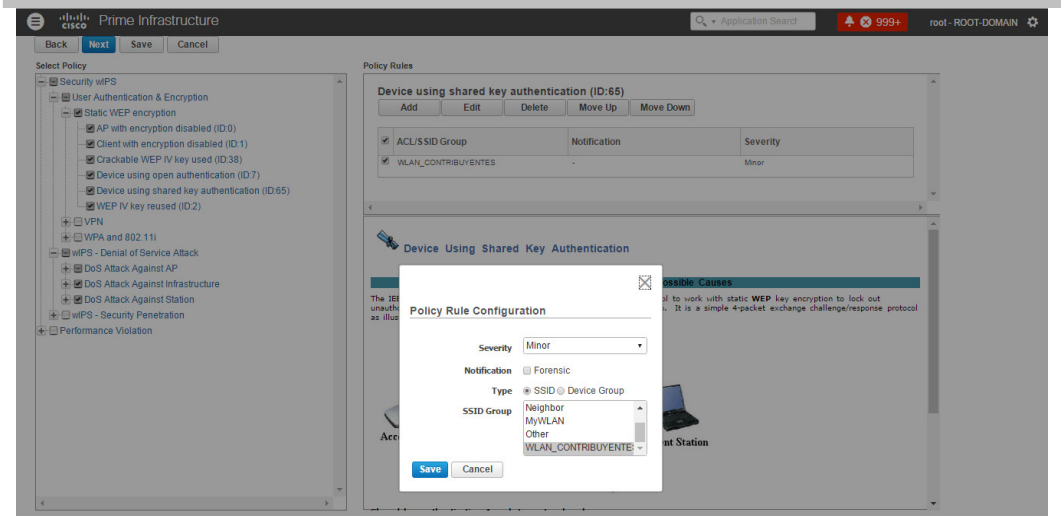


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: USER AUTHENTICATION & ENCRYPTION

POLÍTICA: STATIC WEP ENCRYPTION

ALARMA: DEVICE USING SHARED KEY AUTHENTICATION

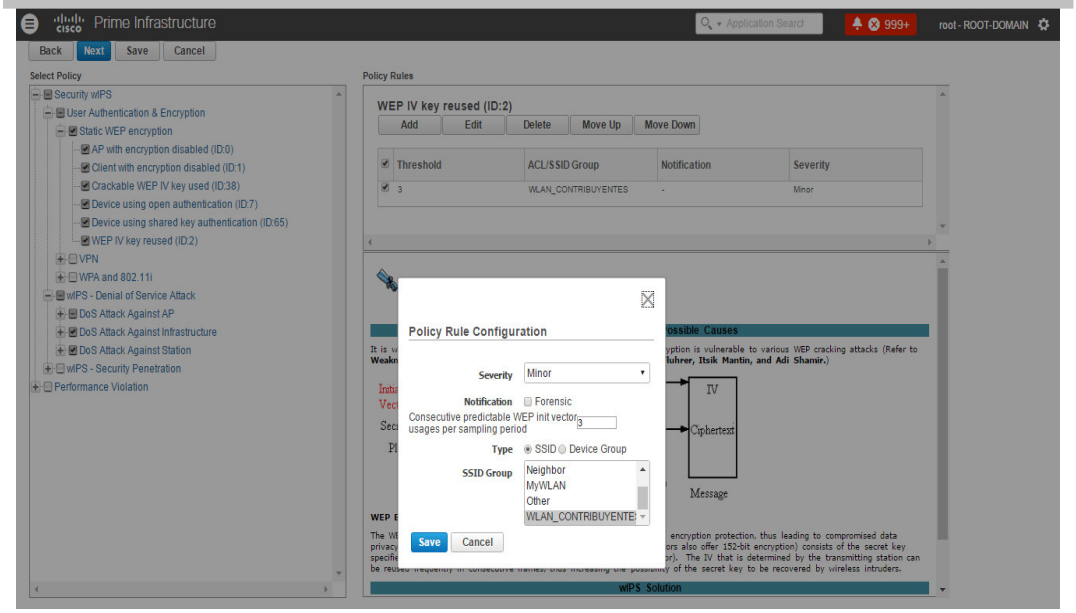


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: USER AUTHENTICATION & ENCRYPTION

POLÍTICA: STATIC WEP ENCRYPTION

ALARMA: DEVICE USING OPEN AUTHENTICATION

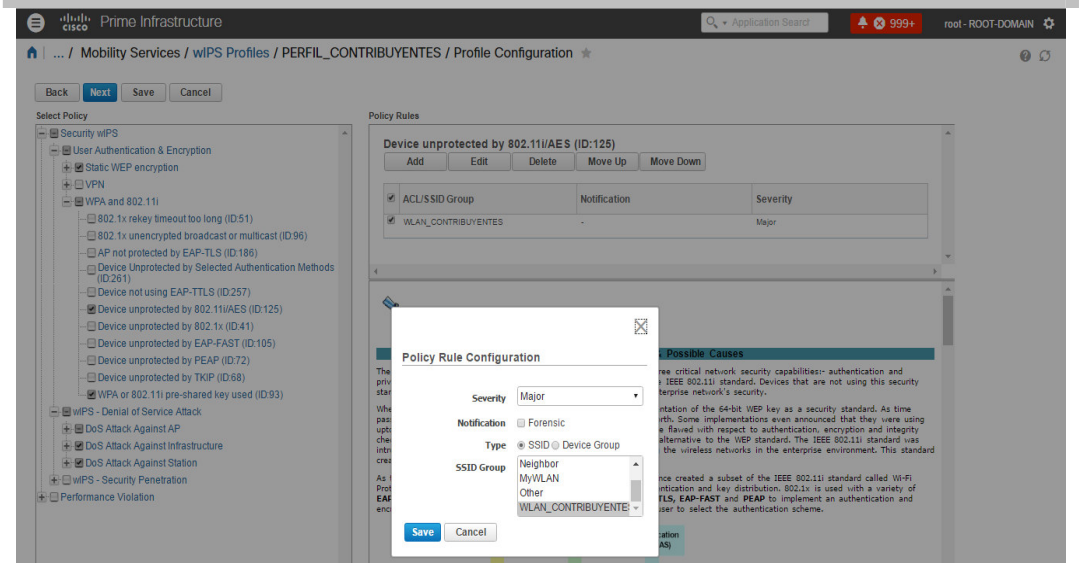


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: USER AUTHENTICATION & ENCRYPTION

POLÍTICA: WPA AND 802.11i

ALARMA: DEVICE UNPROTECTED BY 802.11/AES

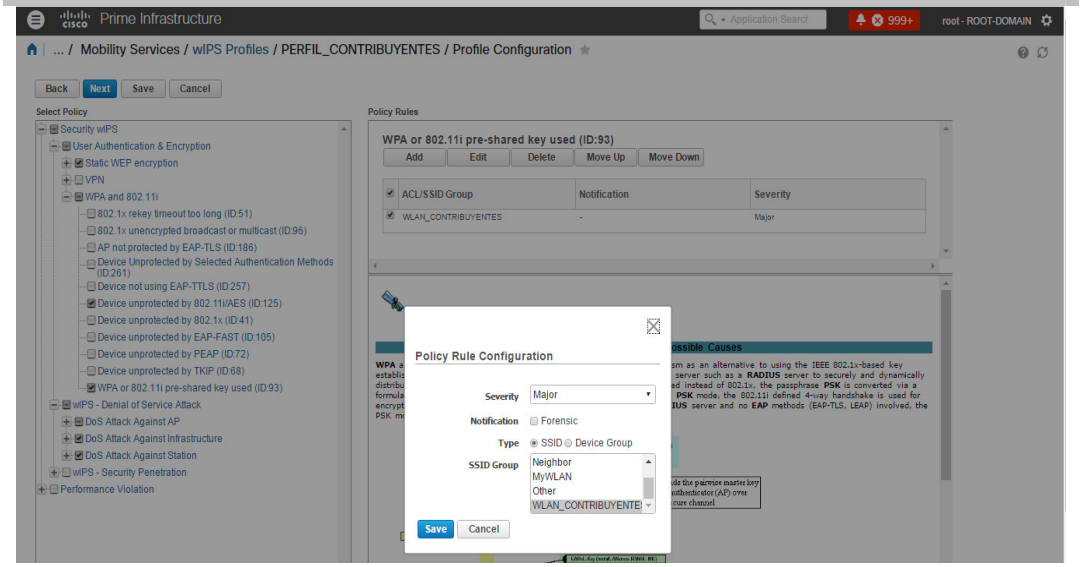


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: USER AUTHENTICATION & ENCRYPTION

POLÍTICA: WPA AND 802.11i

ALARMA: DEVICE UNPROTECTED BY 802.11/AES

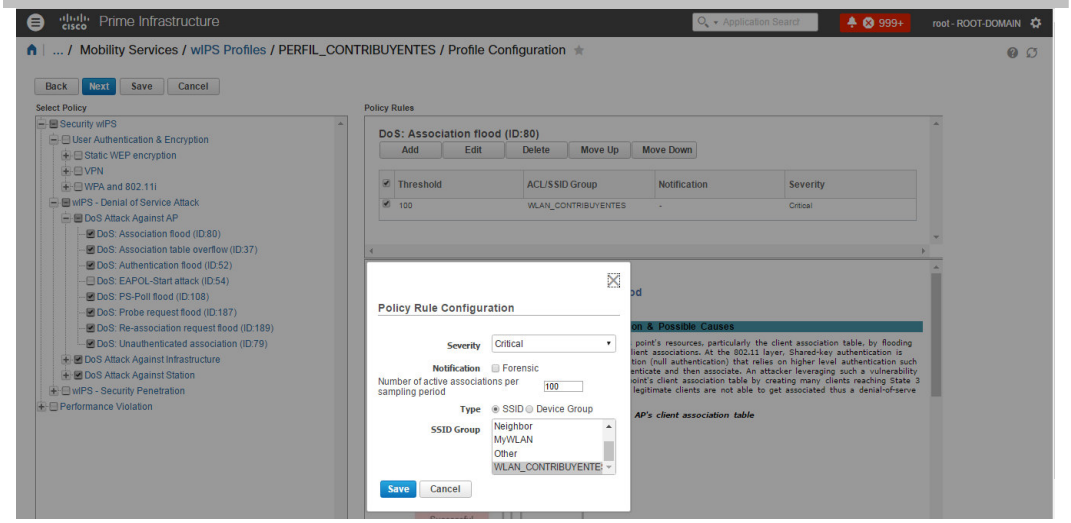


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST AP

ALARMA: DoS ASSOCIATION FLOOD

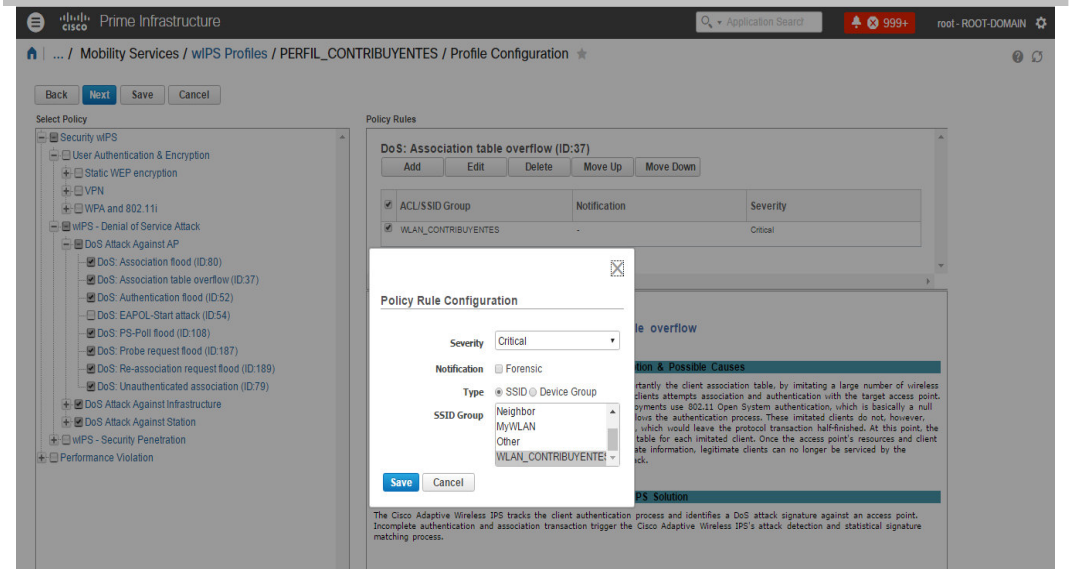


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST AP

ALARMA: DoS ASSOCIATION FLOOD

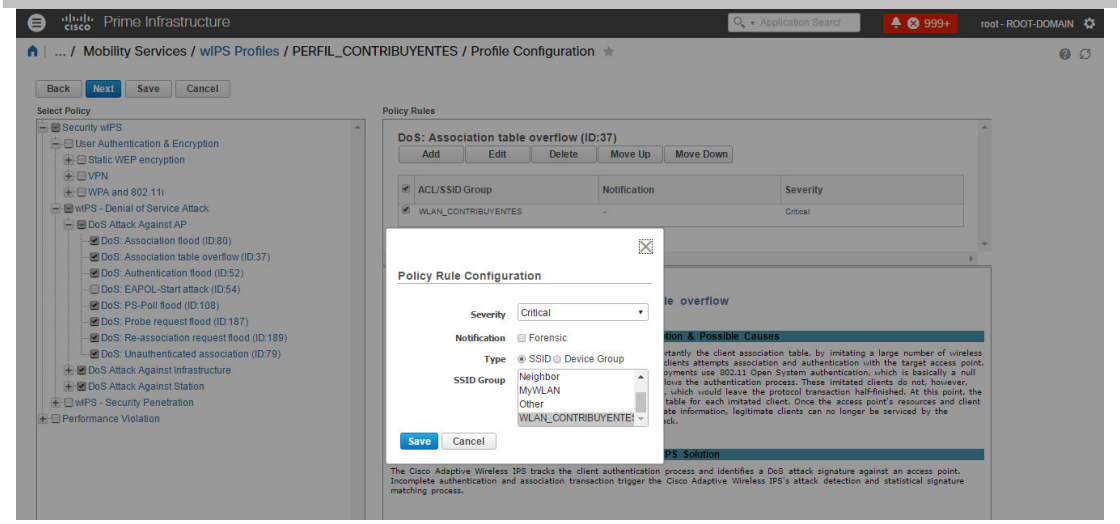


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST AP

ALARMA: DoS ASSOCIATION TABLE OVERFLOW

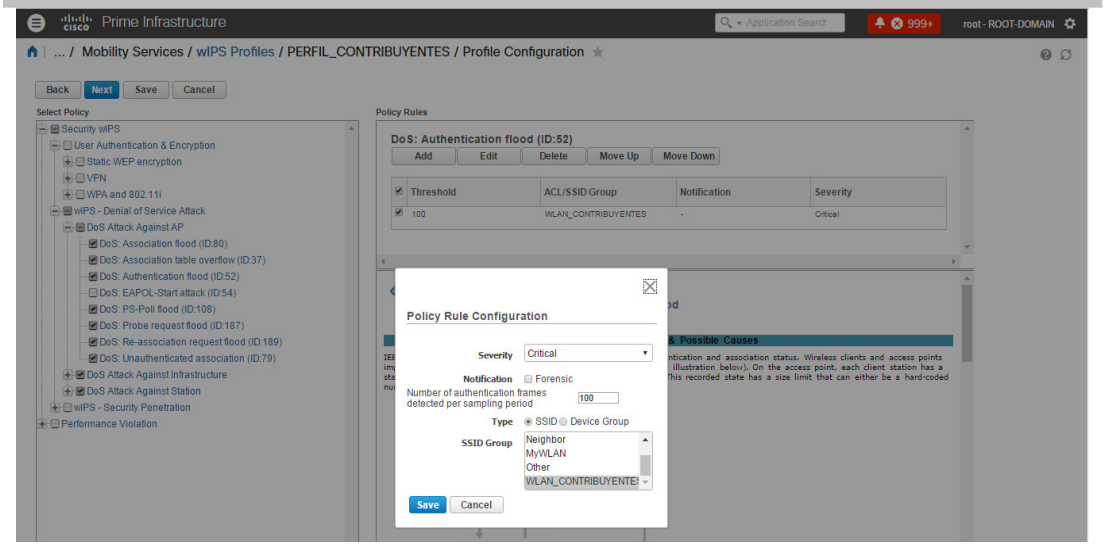


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST AP

ALARMA: DoS AUTHENTICATION FLOOD

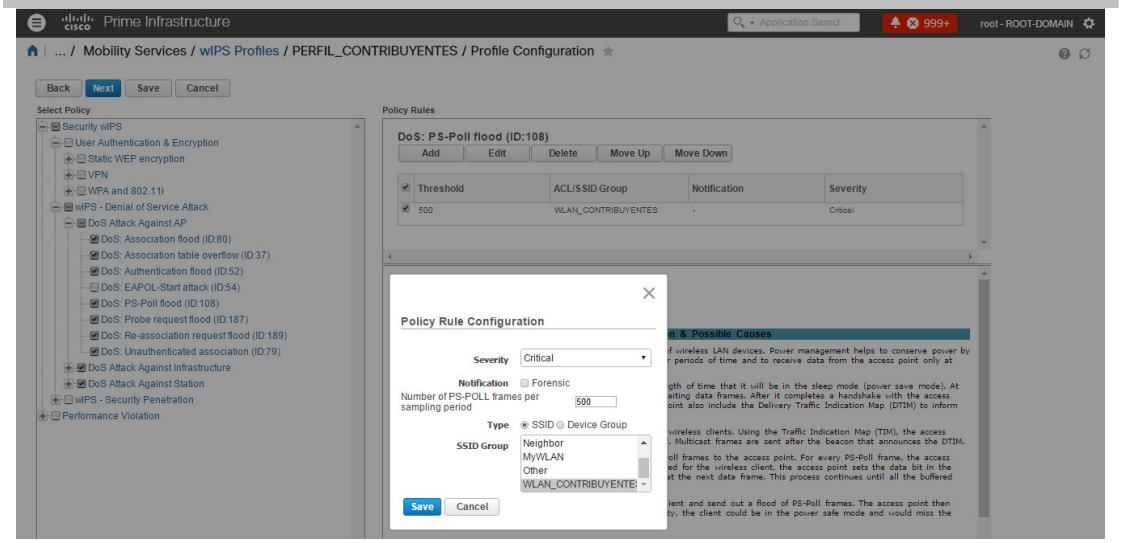


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST AP

ALARMA: DoS PS-POLL FLOOD

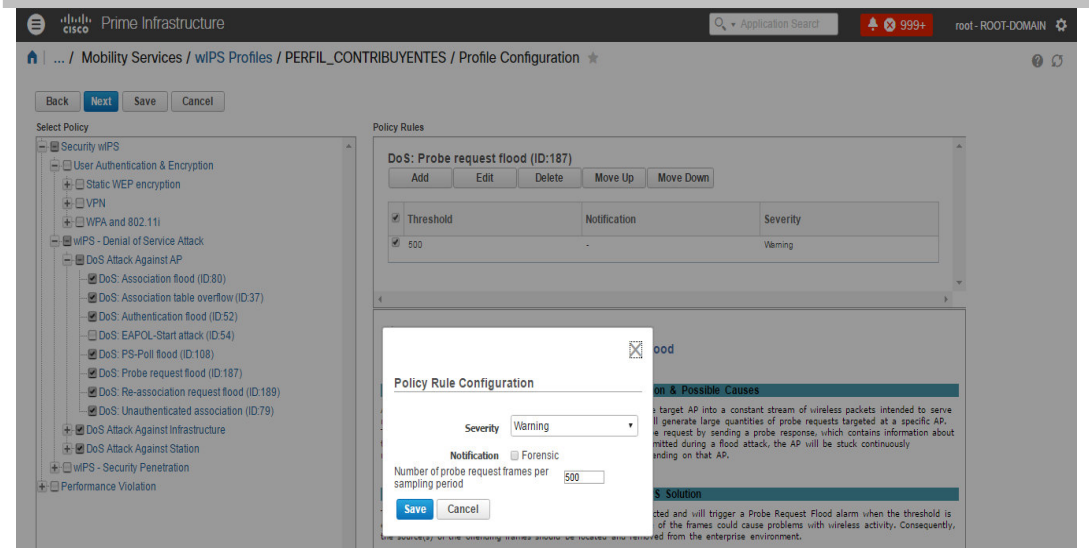


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST AP

ALARMA: DoS PROBE REQUEST FLOOD

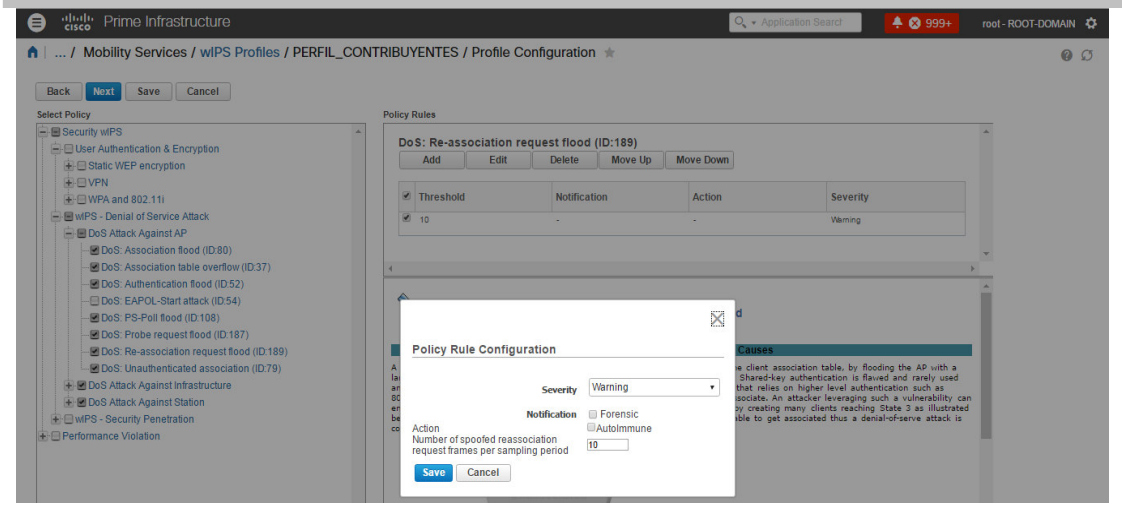


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST AP

ALARMA: DoS RE-ASSOCIATION REQUEST FLOOD

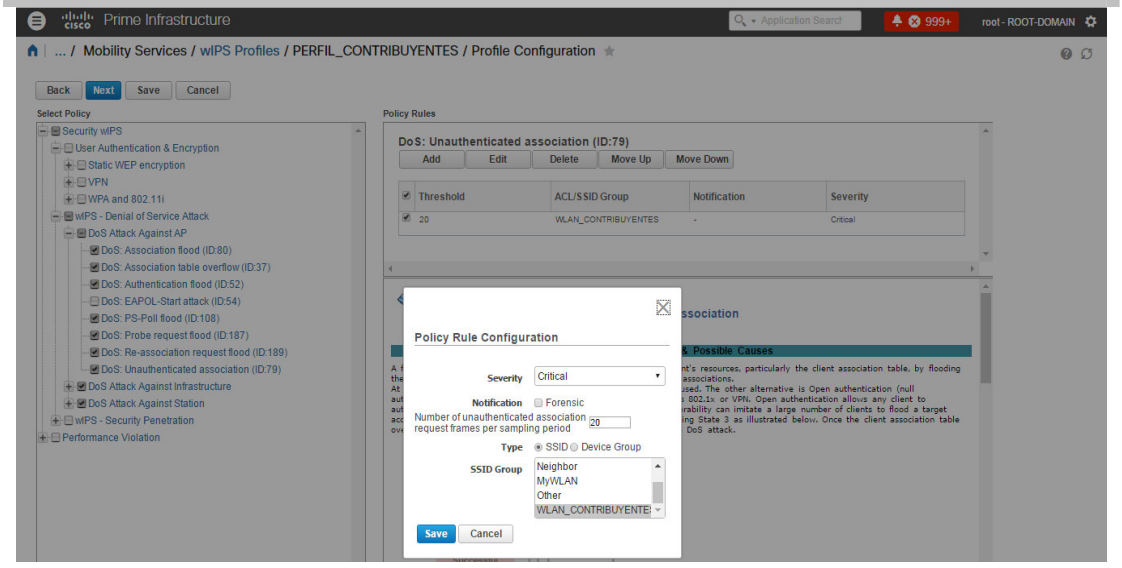


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST AP

ALARMA: DoS UNAUTHENTICATED ASSOCIATION

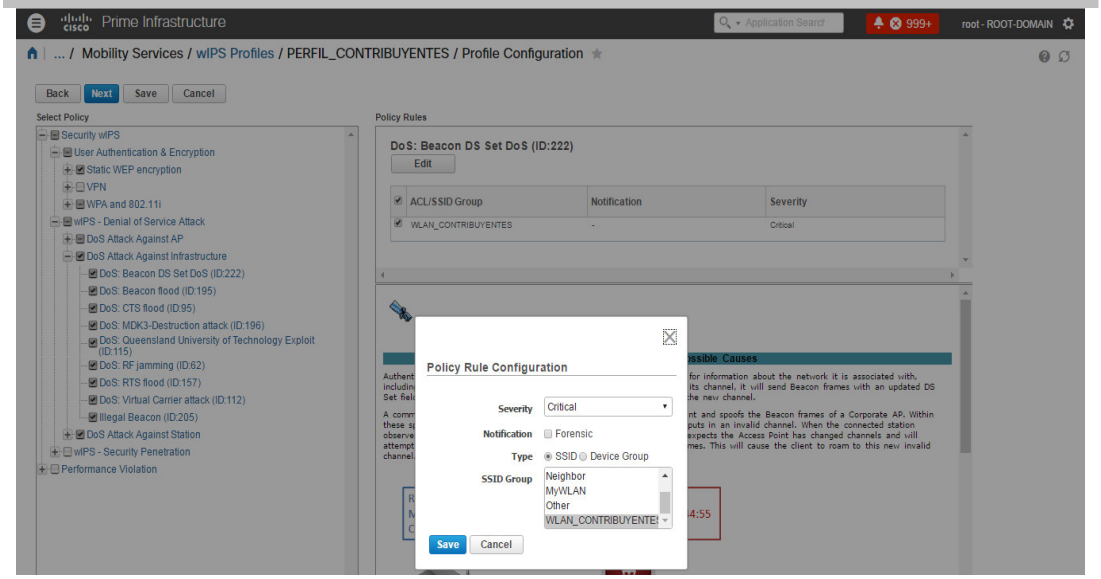


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST INFRASTRUCTURE

ALARMA: DoS BEACON DS SET DoS

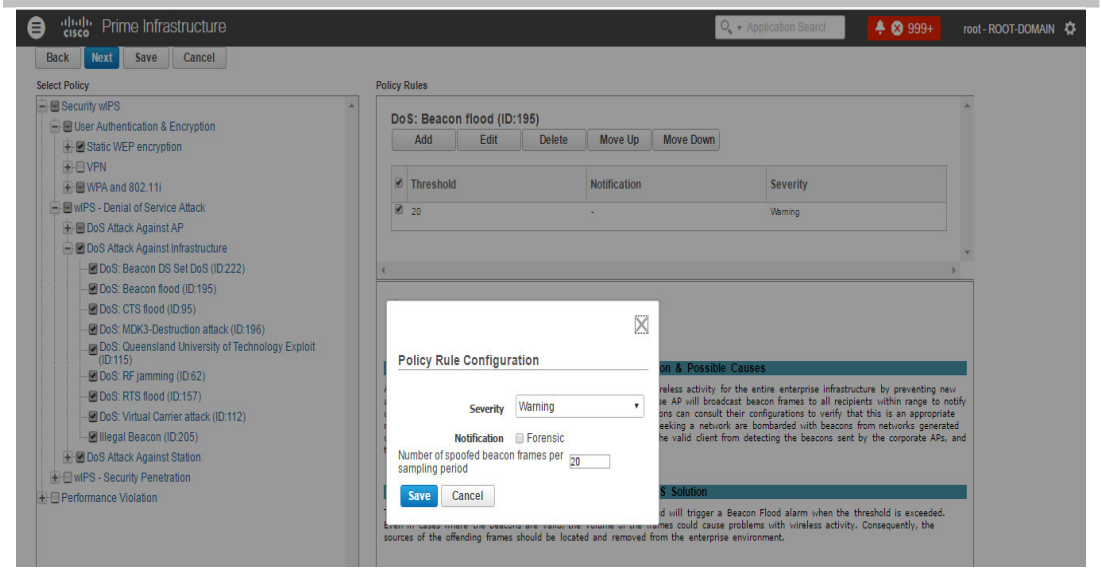


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST INFRASTRUCTURE

ALARMA: DoS BEACON FLOOD

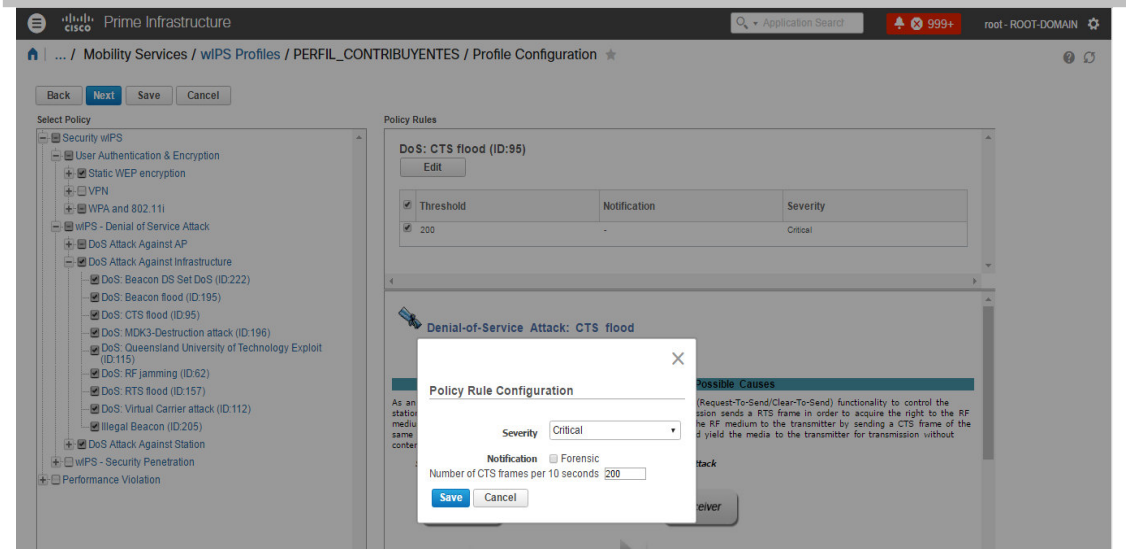


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST INFRASTRUCTURE

ALARMA: DoS CTS FLOOD

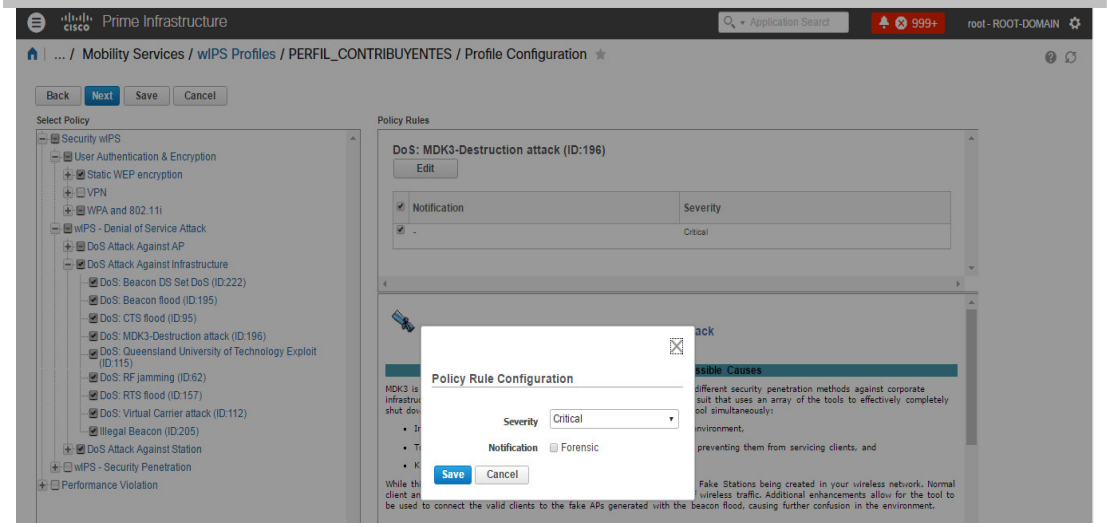


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST INFRASTRUCTURE

ALARMA: DoS MDK3-DESTRUCTION ATTACK

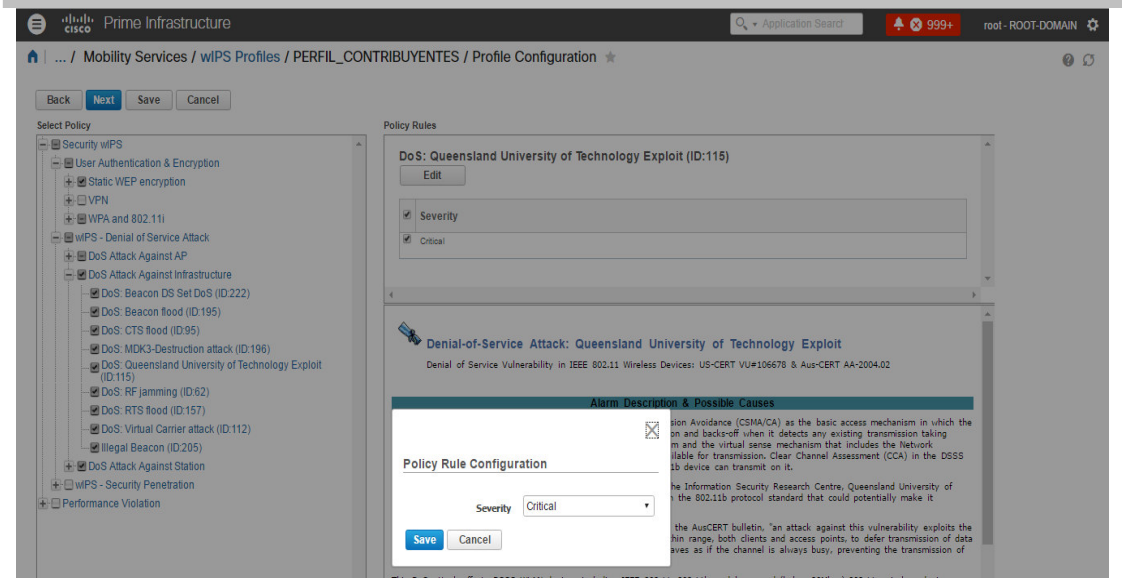


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST INFRASTRUCTURE

ALARMA: DoS QUEENSLAND UNIVERSITY OF TECHNOLOGY EXPLOIT

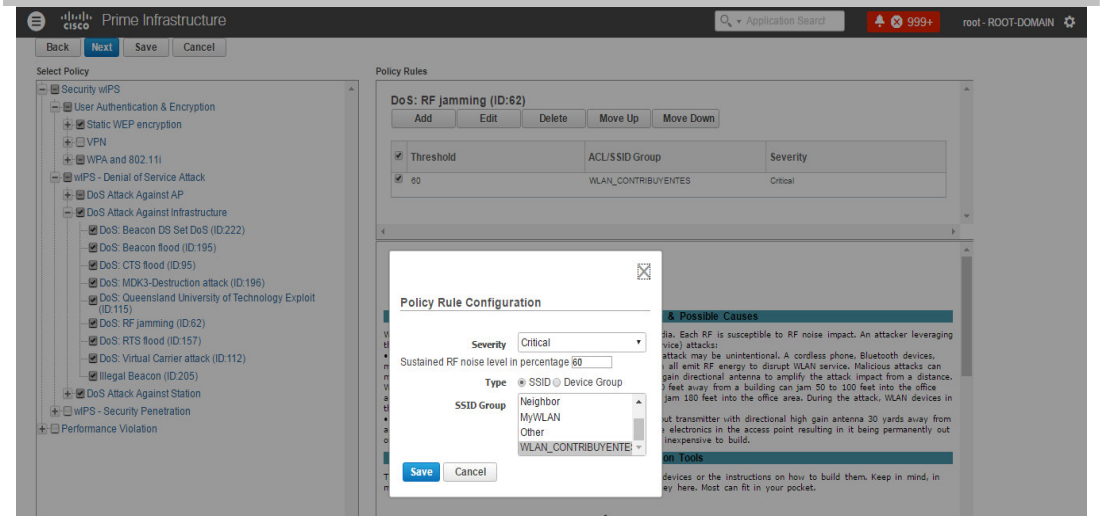


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST INFRASTRUCTURE

ALARMA: DoS RF JAMMING

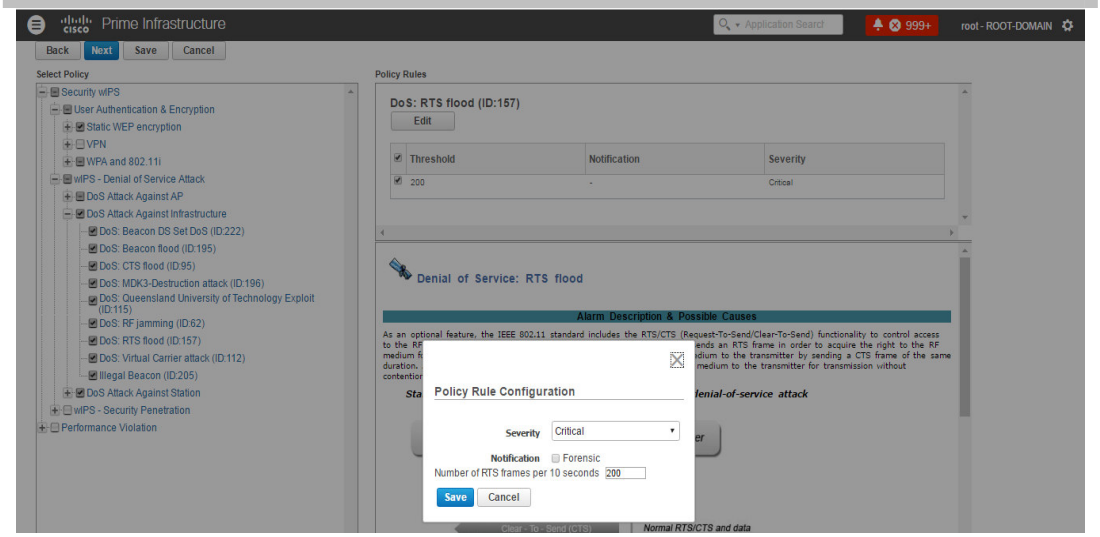


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST INFRASTRUCTURE

ALARMA: DoS RTS FLOOD

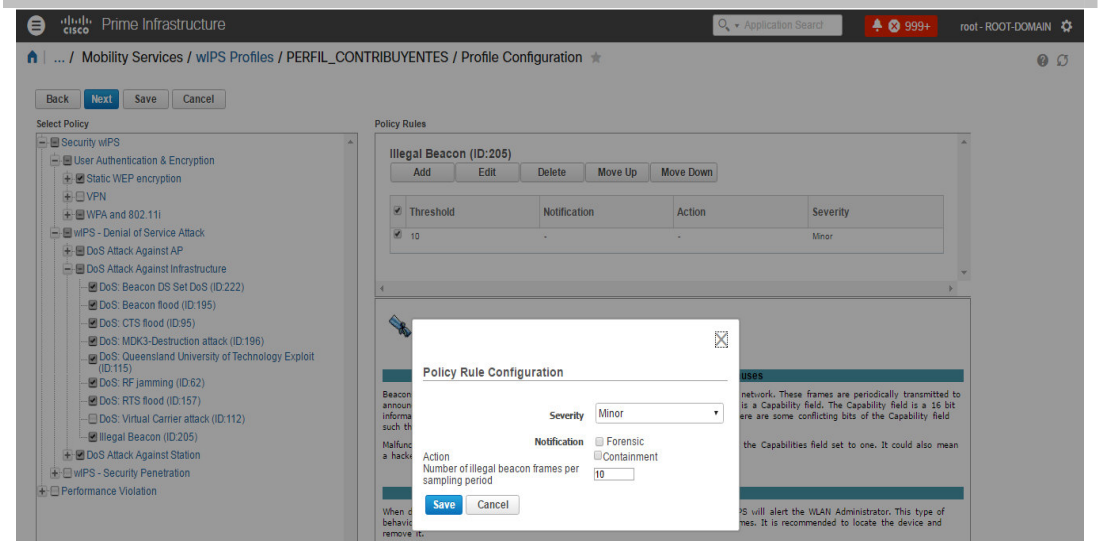


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST INFRASTRUCTURE

ALARMA: ILLEGAL BEACON

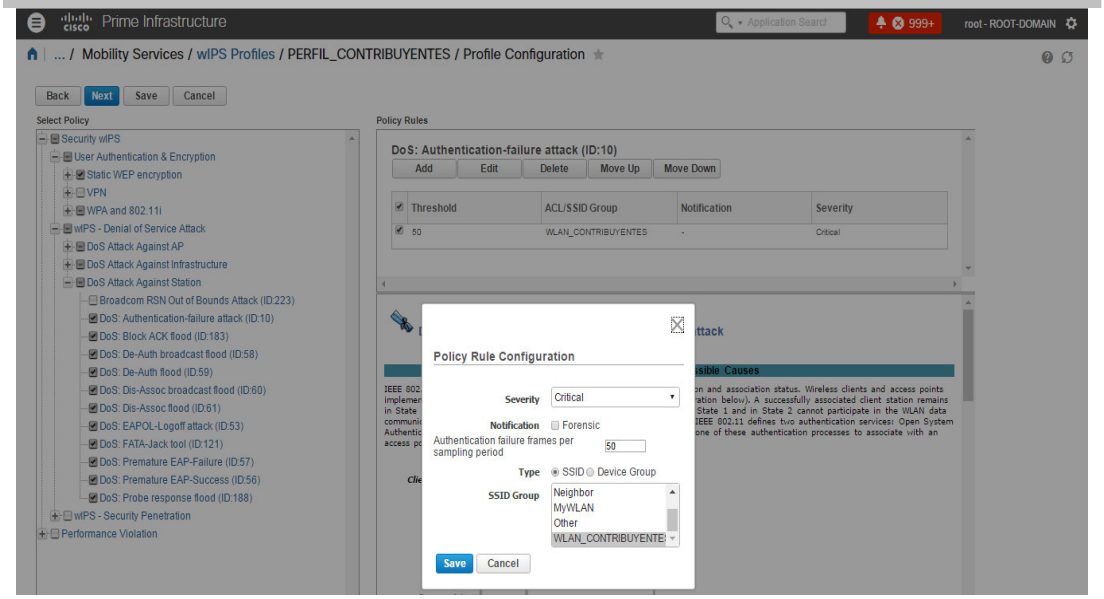


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST STATION

ALARMA: DoS AUTHENTICATION-FAILURE ATTACK

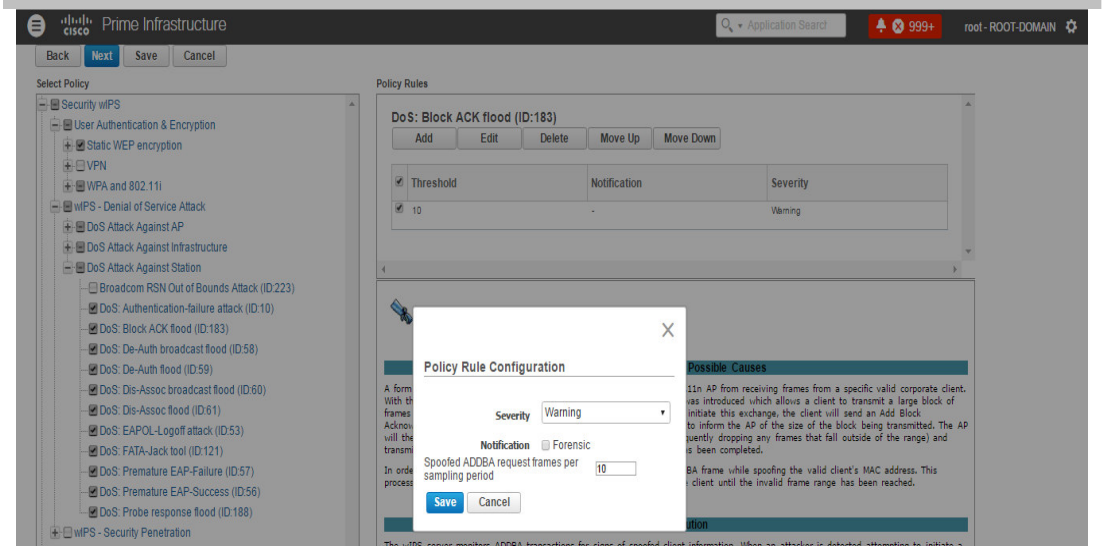


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST STATION

ALARMA: DoS BLOCK ACK FLOOD

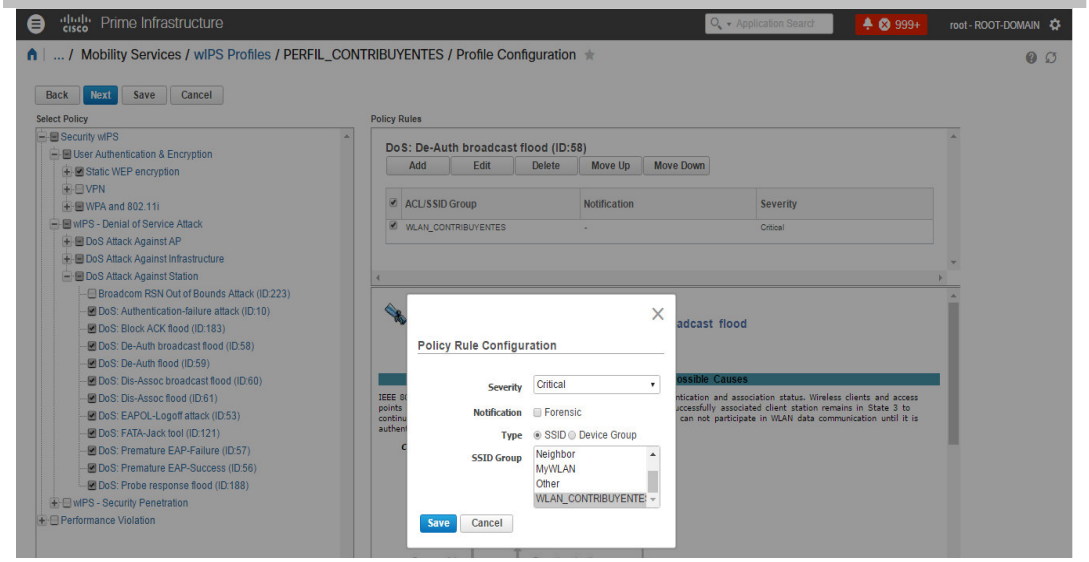


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST STATION

ALARMA: DoS DE-AUTH BROADCAST FLOOD

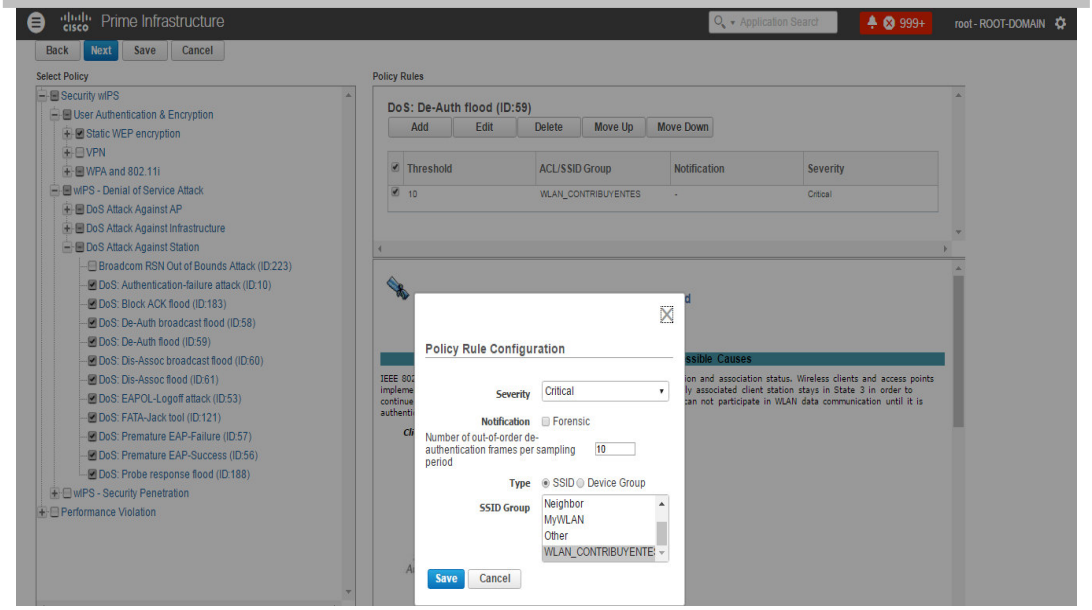


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST STATION

ALARMA: DoS DE-AUTH FLOOD

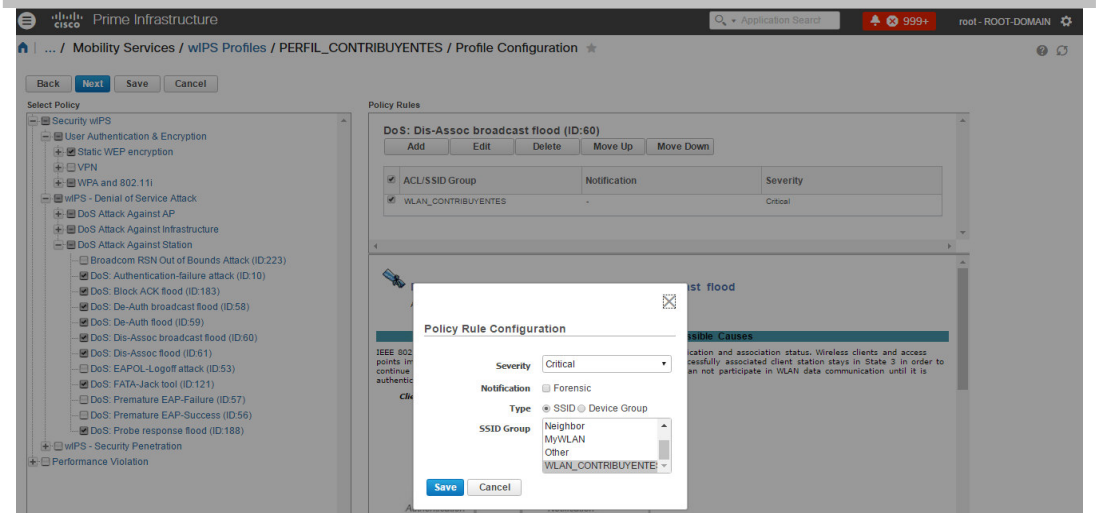


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST STATION

ALARMA: DoS DIS-ASSOC BROADCAST FLOOD

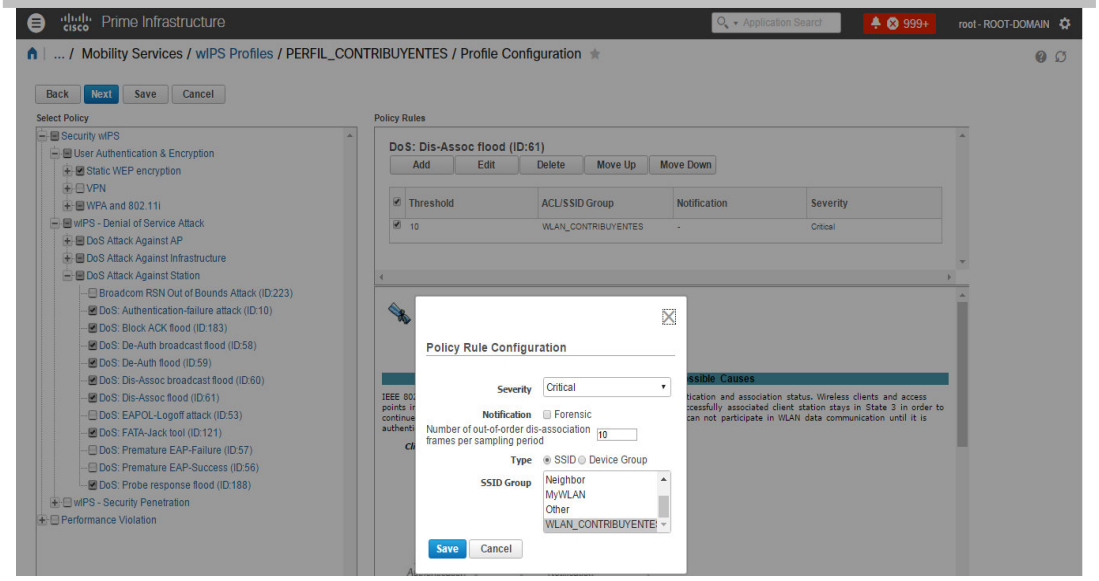


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST STATION

ALARMA: DoS DIS-ASSOC FLOOD

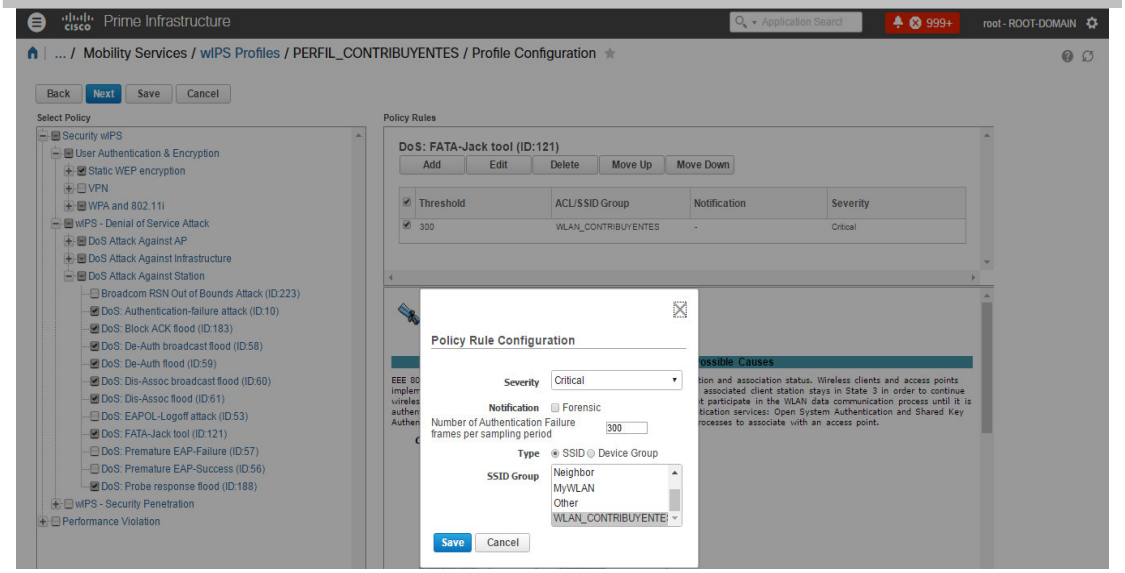


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST STATION

ALARMA: DoS FATA-JACK TOOL

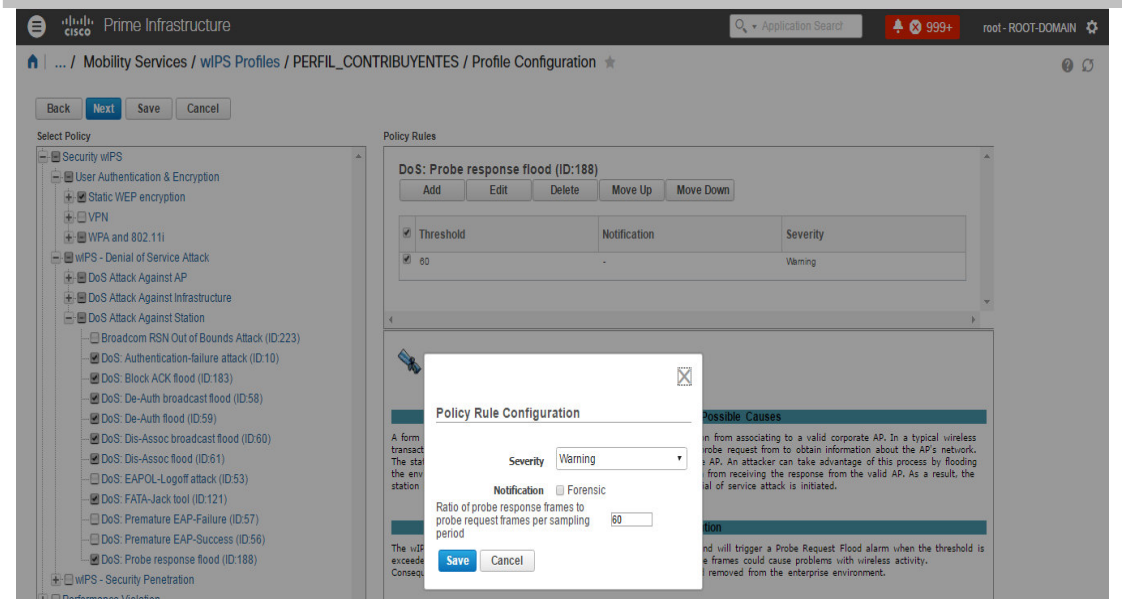


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST STATION

ALARMA: DoS FATA-JACK TOOL

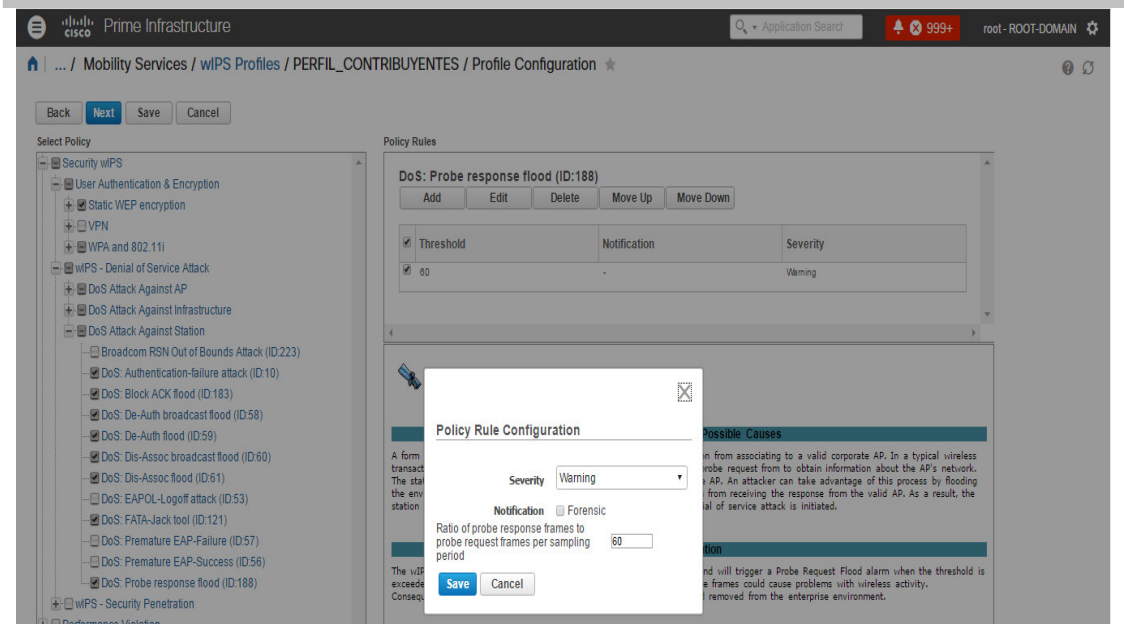


CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – DENIAL OF SERVICE ATTACK

POLÍTICA: DoS ATTACK AGAINST STATION

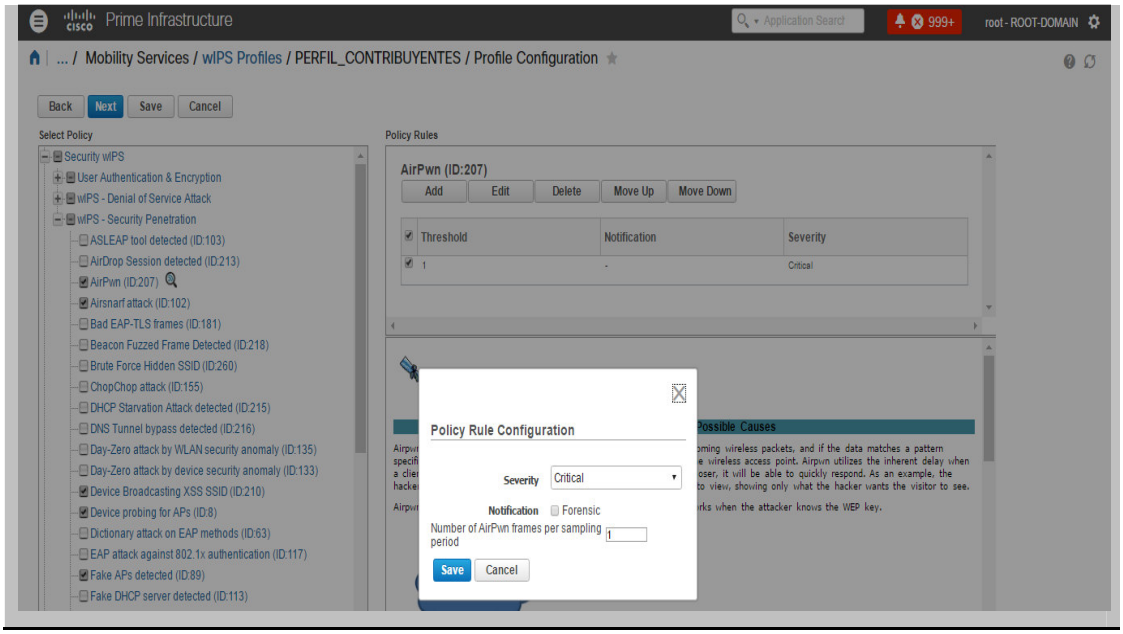
ALARMA: DoS PROBE RESPONSE FLOOD



CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – SECURITY PENETRATION

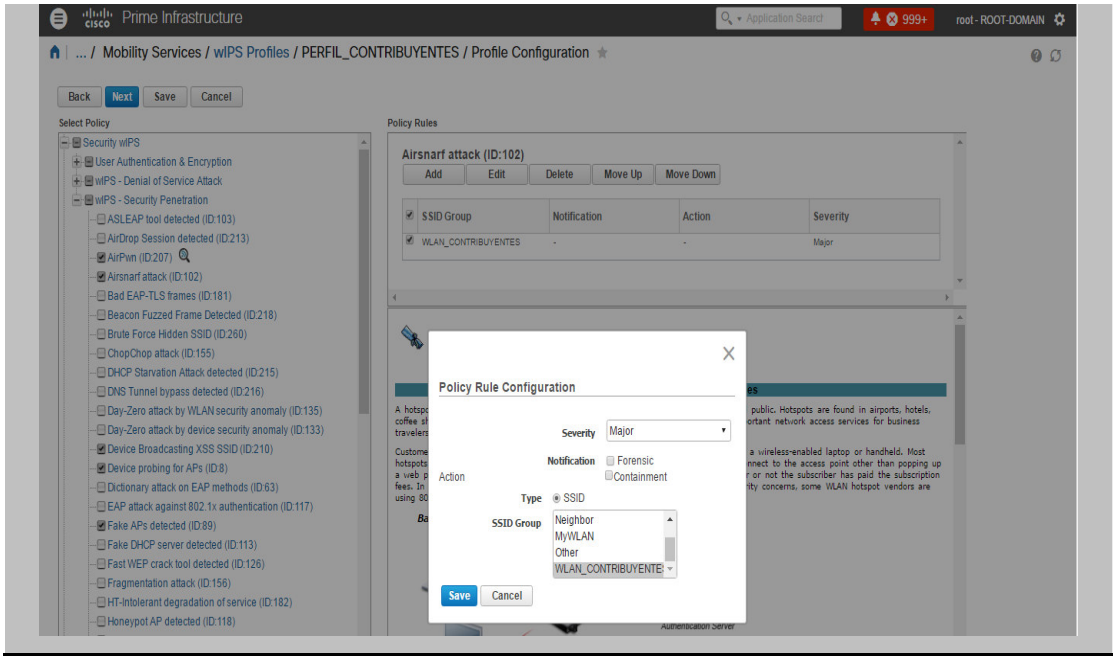
ALARMA: AIRPWN



CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – SECURITY PENETRATION

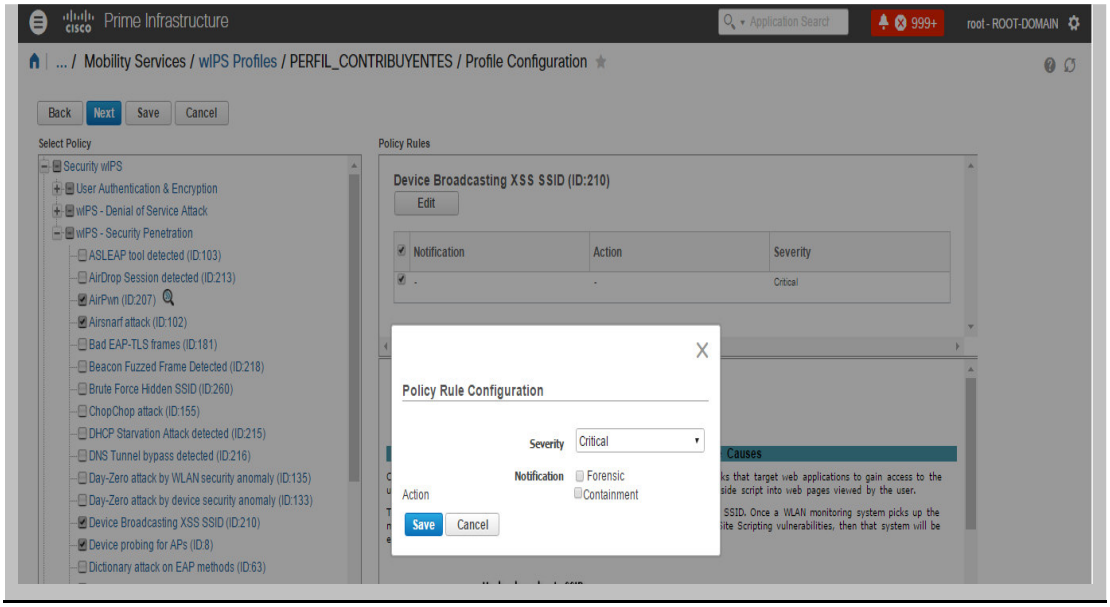
ALARMA: AIRSNARF ATTACK



CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – SECURITY PENETRATION

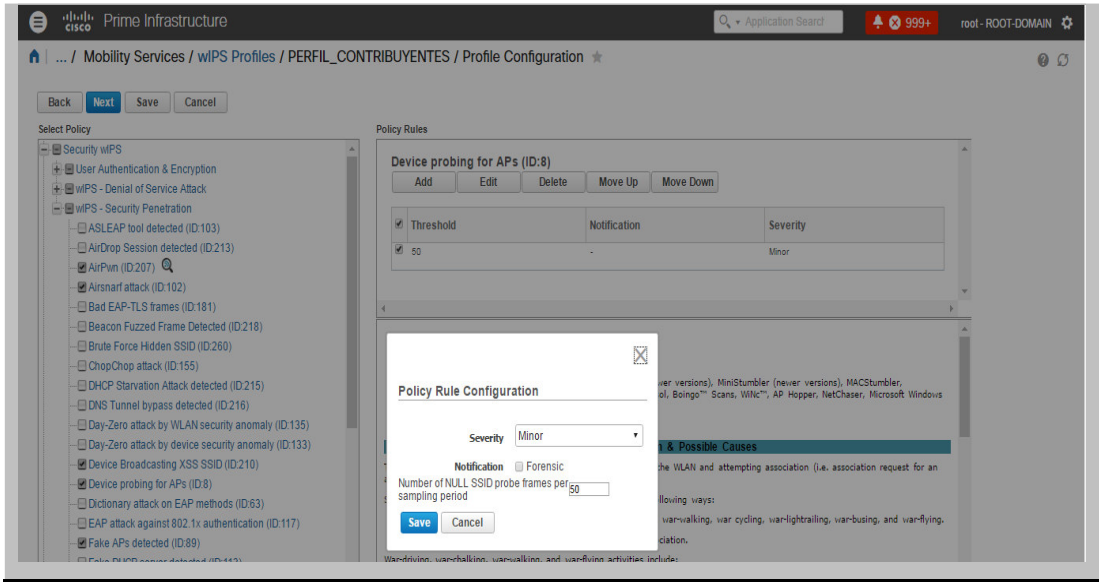
ALARMA: DEVICE BROADCASTING XSS SSID



CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – SECURITY PENETRATION

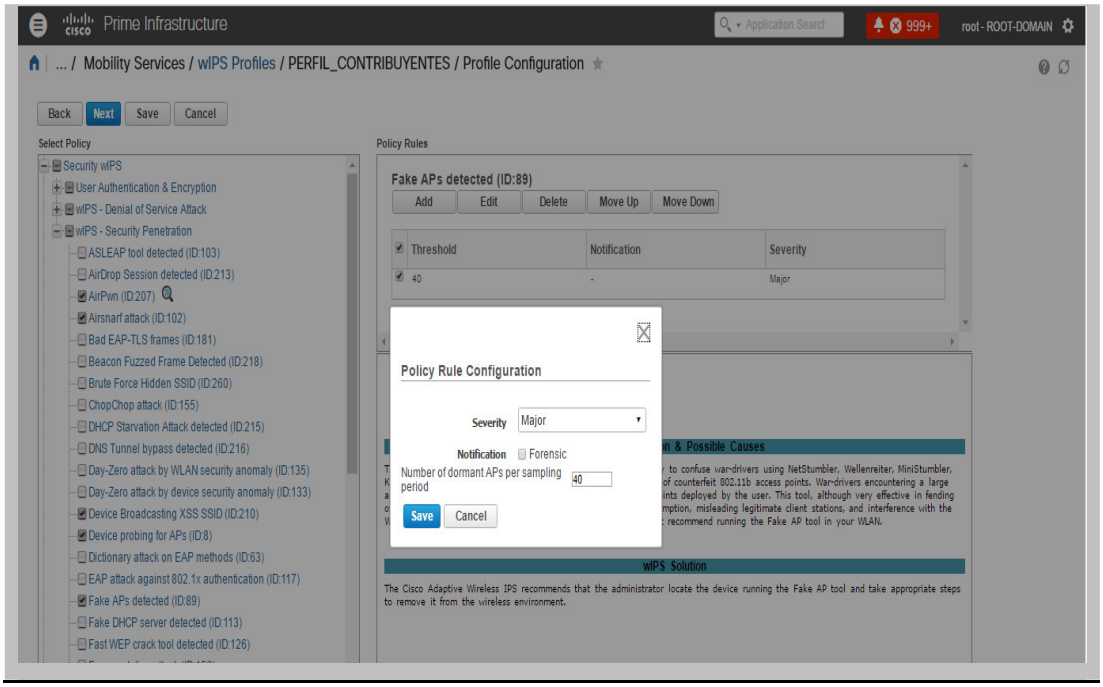
ALARMA: DEVICE PROBING FOR AP's



CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – SECURITY PENETRATION

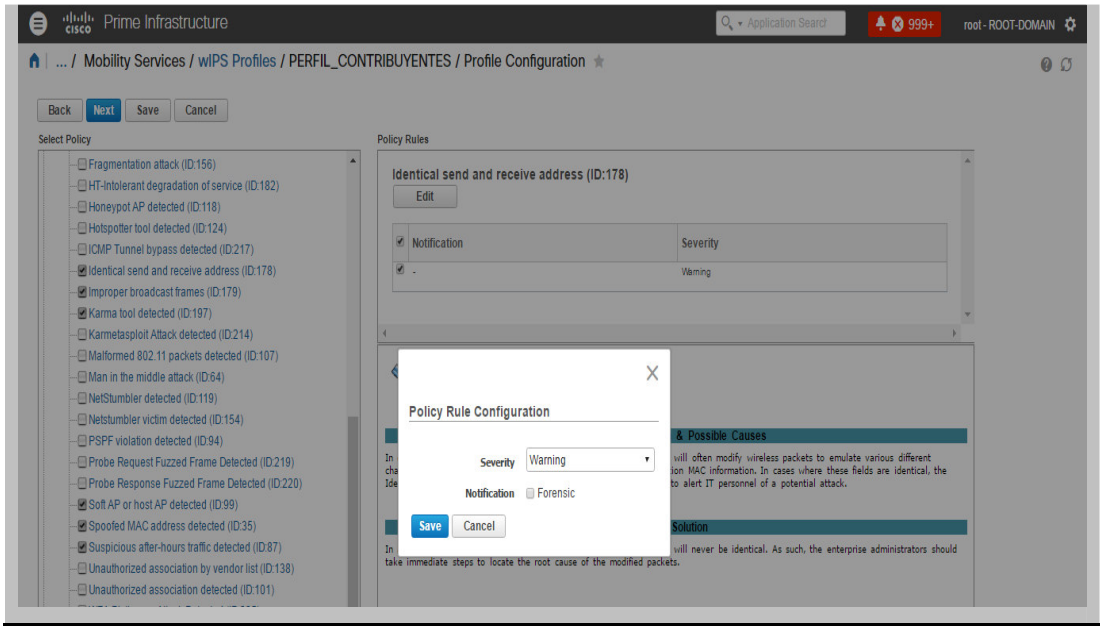
ALARMA: DEVICE PROBING FOR AP's



CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – SECURITY PENETRATION

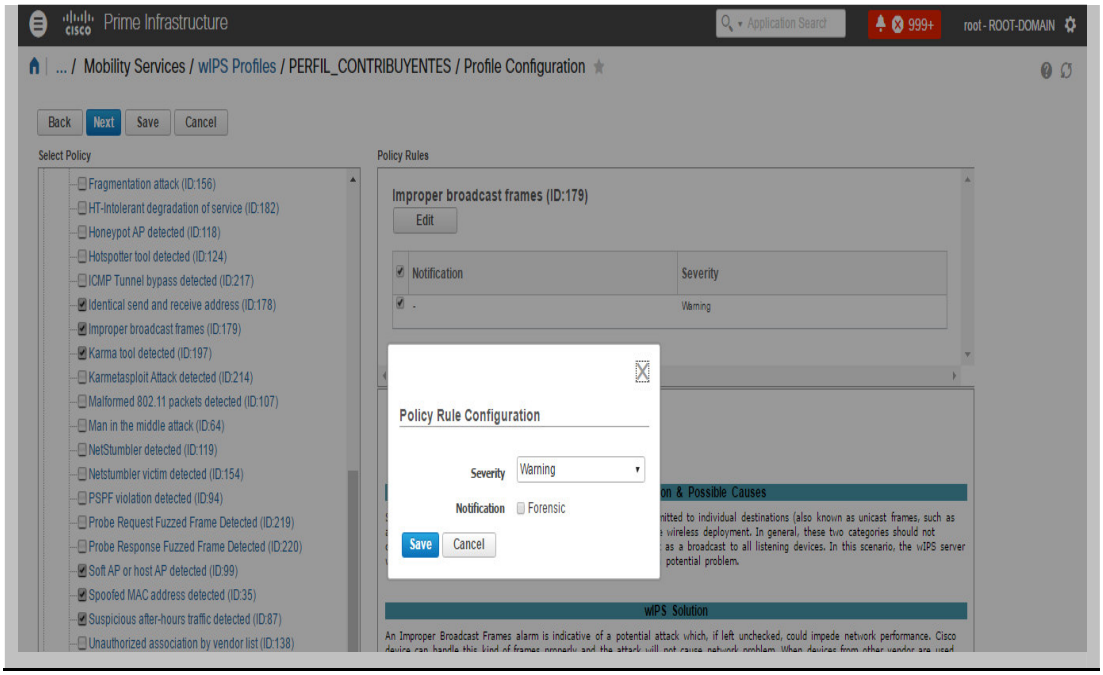
ALARMA: IDENTICAL SEND AND RECEIVE ADDRESS



CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – SECURITY PENETRATION

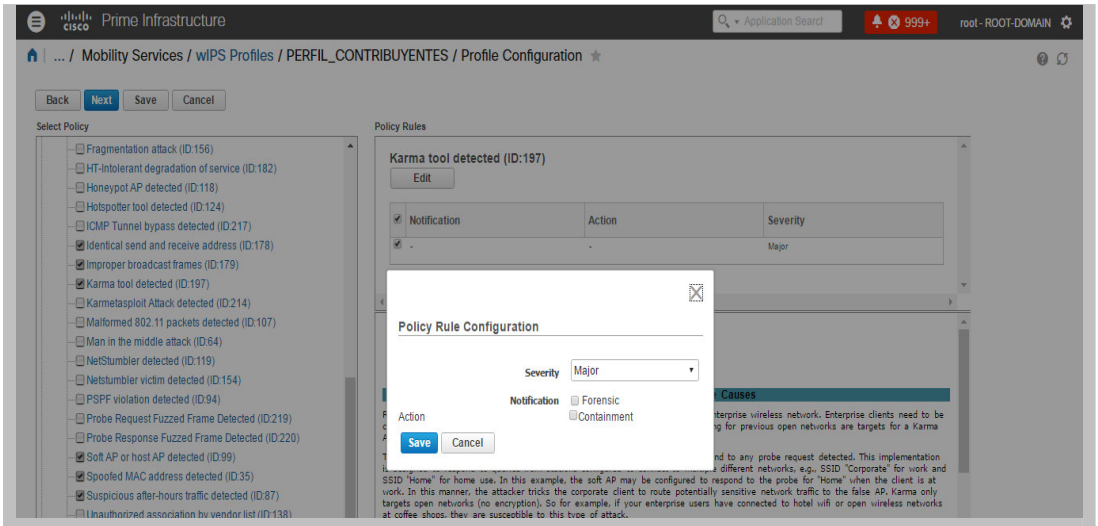
ALARMA: IMPROPER BROADCAST FRAMES



CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – SECURITY PENETRATION

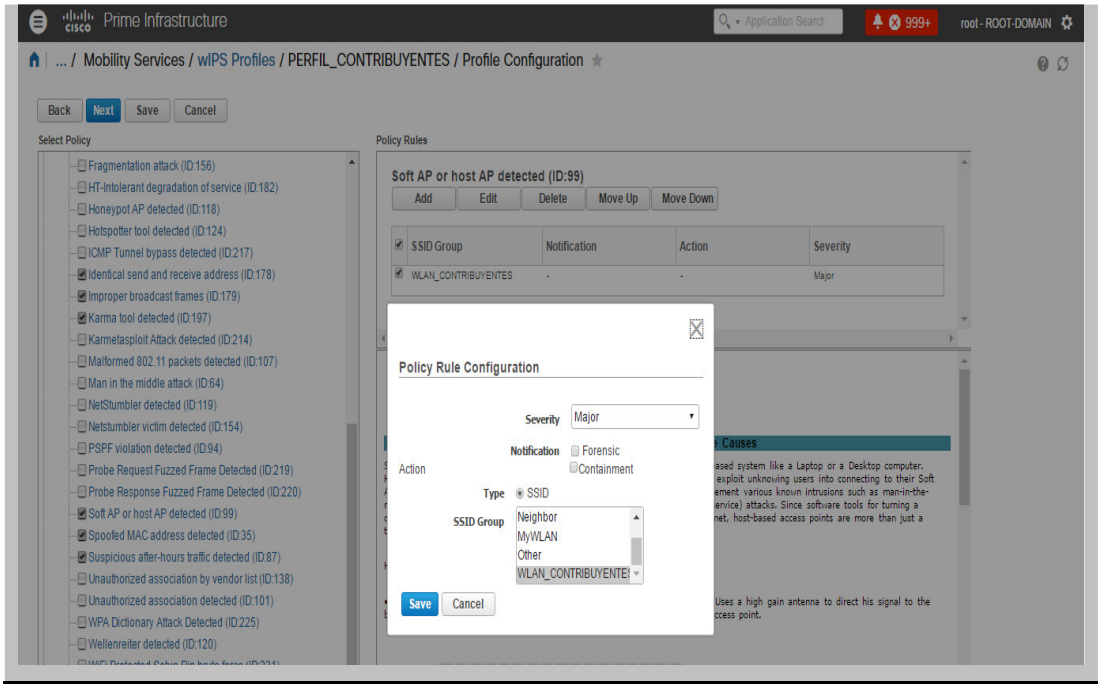
ALARMA: KARMA TOOL DETECTED



CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – SECURITY PENETRATION

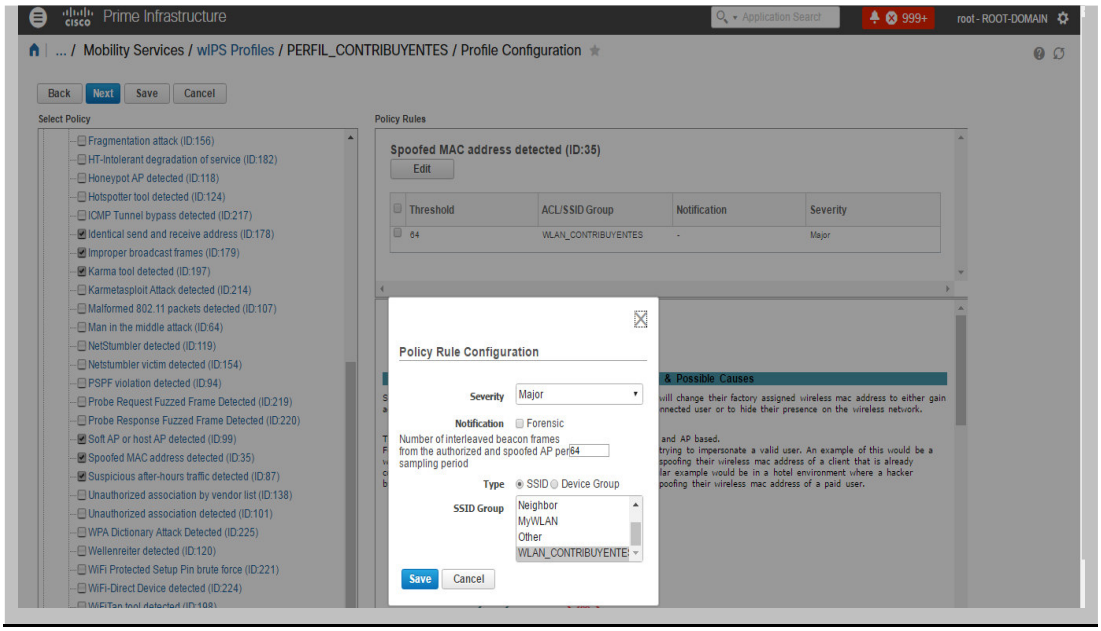
ALARMA: SOFT AP OR HOST AP DETECTED



CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – SECURITY PENETRATION

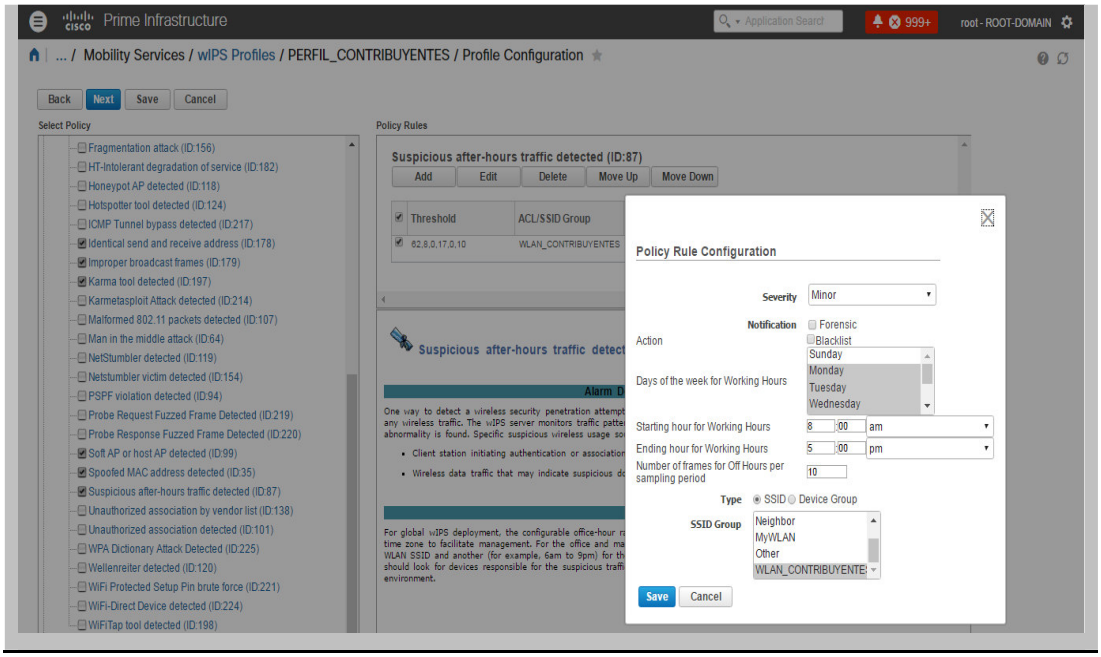
ALARMA: SPOOFED MAC ADDRESS DETECTED



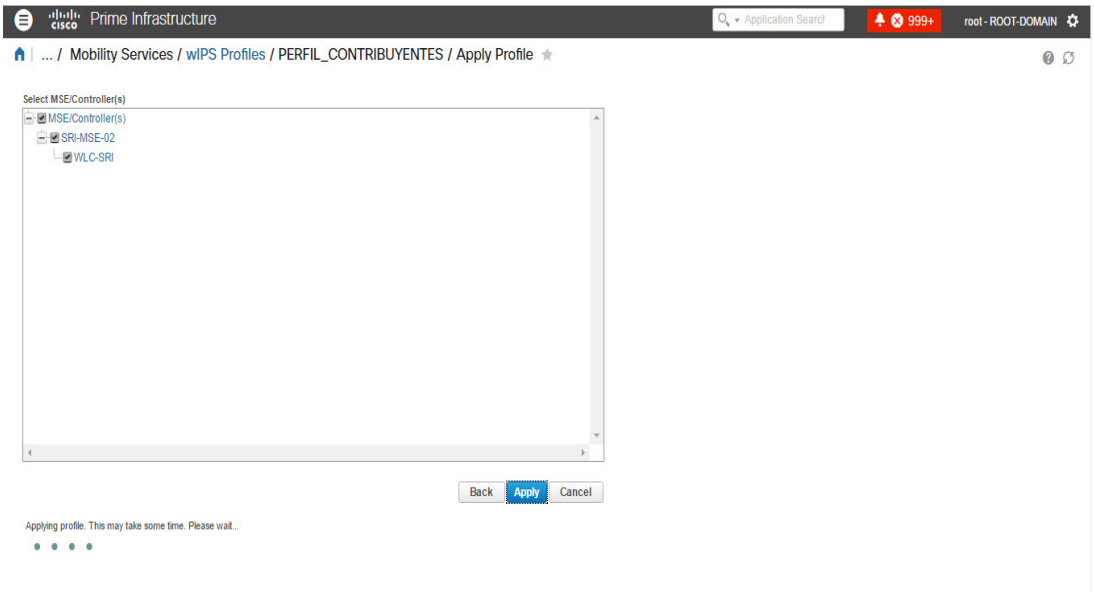
CATEGORIA: SECURITY WIPS

SUBCATEGORIA: WIPS – SECURITY PENETRATION

ALARMA: SUSPICIOUS AFTER-HOURS TRAFFIC DETECTED



e) Configuradas las políticas y alarmas de WIPS es oportuno aplicar todas las configuraciones al SRI-MSE-02 asociado a la controladora WLC. Dicho proceso fue implementado y se lo puede observar en la siguiente imagen.



Anexo 5: Propuesta de Política BYOD

"EMPRESA PÚBLICA DE RECAUDACIÓN DE IMPUESTOS"

Propuesta de Política Bring Your Own Device

Código:	
Versión:	
Fecha de la versión:	
Creado por:	
Aprobado por:	
Confidencialidad:	

HISTORIAL DE MODIFICACIONES

Fecha	Versión	Creado por:	Descripción de la modificación
dd/mm/aa	x.x	[Nombre]	[Descripción básica del documento]

1 Política de Abordaje de Dispositivos Móviles.

La primera política que se contemplará dentro del presente documento es la denominada "On-Boarding Policy" y en ella se darán los lineamientos generales para que el proceso de registro tanto del usuario como del dispositivo móvil del funcionario interno de la "Empresa Pública de Recaudación de Impuestos" pueda llevarse a cabo en función de un acuerdo de uso del esquema BYOD que deberá ser aceptado.

Se entenderán los términos On-Boarding, abordaje y sus similares como sinónimos de conexión de un dispositivo móvil personal sean tablet o Smartphone dentro de un esquema BYOD institucional.

1.1 Objetivo General

Delimitar los mecanismos de conexión que los dispositivos móviles sean tablets o smatphone's propiedad de los funcionarios de la "Empresa Pública de Recaudación de Impuestos" deben adoptar para disponer de acceso a la red inalámbrica institucional.

1.2 Objetivos Específicos.

- Definir el proceso de registro de usuarios.
- Definir el proceso de registro de dispositivos móviles.
- Definir el acuerdo de aceptación de servicios para el usuario.

1.3 Dispositivos Admitidos

Para efectos de garantizar conexión a la mayor parte de dispositivos móviles de propiedad de los funcionarios, a continuación se describen las características de S.O. y versión de los mismos que se deberán cumplir previos a acceder al esquema BYOD propuesto.

S.O.	VERSIÓN	CANTIDAD POR USUARIO
IOS	5.0 y superior	1
ANDROID	3.2 y superior	1

Tabla 1. Características de Dispositivos admitidos dentro de esquema BYOD institucional.

1.2.1 Proceso de Registro de usuarios.

a) Los funcionarios que adopten el esquema BYOD deberán conectarse a la red inalámbrica BYOD institucional en donde se les solicitarán información personal que permita identificarlos de manera obligatoria. Para este punto se deberán considerar los lineamientos indicados en la (*política de identificación y control de accesos)*.

b) Los mecanismos que se proponen para el proceso de registro serán el Portal de Autoregistro o el portal BYOD.

c) Para el caso de los funcionarios el proceso de registro será opcional, aclarando que deberán ingresar sus credenciales internas con el afán de ser redirigidos a la etapa de registro del dispositivo.

d) El portal de autoregistro deberá ser utilizado en aquellos casos en los cuales funcionarios de otras instituciones accedan a las inmediaciones de la "Empresa Pública de Recaudación de Impuestos".

e) Respecto al punto d, se deberá prever un perfilamiento que garantice únicamente navegación hacia internet, mas no a los recursos institucionales de información.

1.2.2 Proceso de Registro de Dispositivos.

a) Completada la etapa de registro de cuenta de usuario, el registro del dispositivo implicará proveer de información referente a: marca, modelo, IMEI, etc.

b) Los datos de mac addres son parte de la información de contexto que automáticamente la plataforma CISCO ISE asignará al dispositivo como un ID único que permita identificarlo en la red.

1.2.3 Proceso de Aceptación de Uso / Usuario Final.

a) El proceso de aceptación de uso para el usuario final será una interface GUI propia de la plataforma CISCO ISE que se deberá personalizar y que establece la aceptación del acuerdo del funcionario para las condiciones de uso del esquema BYOD que la empresa provee. Los siguientes aspectos serán los mínimos considerados:

    a. El acuerdo de aceptación de uso deberá estar definido en idioma español e incluir un mecanismo que intente garantizar que el funcionario lea todo el acuerdo.

b. El presente acuerdo deberá ser mostrado cada cierto periodo de tiempo establecido inicialmente cada siete días.

c. Confidencialidad de la información.

d. Uso de la red e infraestructura institucional para efectos laborales y no para actividades fuera de lo normal o que pongan en algún tipo de riesgo, amenaza o vulnerabilidad a la seguridad de la infraestructura tecnológica institucional.

e. Aceptación de que su dispositivo, aplicaciones y demás parámetros sean monitoreado mediante mecanismos internos institucionales en donde no se comprometa la información personal almacenada en dicho dispositivo.

f. Aceptación de disponibilidad de acceso al dispositivo cuando se requiera para efectos de procesos investigativos relacionados a temas legales internos o externos.

g. El acceso a los recursos de la institución deberán realizarse dentro del entorno institucional y en horarios laborales salvo aquellos casos en donde se justifique la necesidad de hacerlo fuera de horario.

h. El dispositivo que se apegue al esquema BYOD institucional deberá ser utilizado para actividades netamente laborales y personales sin recaer en el acceso a navegación inapropiada, de índole sexual o afines.

b) Una vez cumplido la etapa de aceptación de uso por parte del usuario final la política de abordaje se dará por cumplida.

c) Para aquellos casos en los cuales por alguna circunstancia no se ejecute el proceso correctamente y se presenten problemas para el registro del dispositivo, estos deberán pasar en primera instancia por un proceso de actualización por parte del propietario del dispositivo y por otra parte deberán contar con la ayuda del área de Redes de la "Empresa Pública de Recaudación de Impuestos" para resolver cualquier eventualidad.

2 Política de Identificación y Control de Acceso.

En la presente política se darán los lineamientos generales para que el manejo de la seguridad de la información y la administración de la privacidad sean gestionadas de manera eficiente. El funcionario que adopte el esquema BYOD propuesto en la "Empresa Pública de Recaudación de Impuestos" deberá respetar los lineamientos estipulados a continuación.

2.1 Objetivo General

Definir los mecanismos que garanticen la seguridad y la privacidad de los funcionarios que adopten el esquema BYOD mediante dispositivos móviles sean tablet's o smatphone's de propiedad de los funcionarios de la "Empresa Pública de Recaudación de Impuestos" haciendo uso de métodos como identificación, autorización y contabilidad.

2.2 Objetivos Específicos.

- Definir lineamientos para implementación de passwords.
- Definir lineamientos que permitan autenticar un usuario BYOD.
- Definir lineamientos que permitan autorizar un usuario BYOD.
- Definir parámetros que permitan disponer de un registro documentado de conexiones tanto de usuarios como dispositivos BYOD.
- Delimitar la segmentación de la red y su alcance.

2.2.1 Passwords.

Para efectos de garantizar un nivel de seguridad en lo referente a claves, contraseñas o passwords para los sistemas, aplicaciones y demás plataformas que dentro del esquema BYOD se vayan a utilizar es permitente considerar los siguientes lineamientos:

a) Los parámetros de complejidad y condiciones que debe cumplir una clave, deberán ser determinados en la plataforma CISCO ISE.

b) Una clave deberá contar con un mínimo de 8 caracteres.

c) Los caracteres utilizados deberán contener mayúsculas, minúsculas, por lo menos un número y un carácter especial como: !, @, #, %, $.

d) La clave deberá tener un tiempo de vigencia de máximo 90 días y se deberá validar que no pueda ser repetida en futuras ocasiones.

e) La inactividad del dispositivo deberá ser controlada mediante un bloqueo del dispositivo considerando un tiempo máximo sugerido de 10 minutos.

f) Se sugiere establecer un máximo de tres intentos fallidos posterior a lo cual, acciones como borrado de datos corporativos pueda ser efectuado de manera automática. Este aspecto se lo considera para un escenario en el cual el dispositivo BYOD haya sido puesto de alguna manera fuera del alcance del propietario.

2.2.2 Autenticación.

a) La autenticación podrá ser realizada mediante mecanismo multi factor para el usuario y el dispositivo BYOD. En este sentido se detalla a continuación los mecanismos que permitirán realizar la autenticación de dispositivos y usuarios BYOD.

b) Los usuarios BYOD contarán con un factor de autenticación provisto mediante su usuario y contraseña y ésta última deberá cumplir con los lineamientos descritos en el apartado destinado a ello y descrito anteriormente.

c) La autenticación para los dispositivos BYOD utilizarán un factor de posesión que incluye la creación e instalación de un certificado digital e intercambiado con la plataforma CISCO ISE para su identificación.

d) El uso del certificado digital será restringido únicamente al dispositivo personal que se autoriza su uso dentro del esquema BYOD.

2.2.3 Autorización.

a) La autorización define el nivel de privilegio y acceso que un usuario BYOD tiene para los sistemas y recursos institucionales.

b) Será autorizado aquel usuario BYOD que por una parte provea credenciales de usuario y contraseña válidos y legítimos y que por otra parte su dispositivo cuente con el certificado digital concebido en el presente documento como un mecanismo de autenticación basado en posesión.

c) Los niveles de acceso se parametrizarán en la plataforma CISCO ISE en donde mediante VLAN's o ACL's puede ser diferenciado el tipo de acceso para cada usuario o grupo.

d) Se deberá contar con la documentación adecuada de ACL's y VLAN's que especifiquen los permisos que representan.

e) Se deberá configurar el perfilamiento adecuado para cada tipo de usuario o grupo de usuarios en la plataforma CISCO ISE.

2.2.4 Contabilidad.

a) La plataforma CISCO ISE deberá contar con las configuraciones necesarias para visualizar las actividades y recursos accedidos por cada uno de los usuarios y dispositivos BYOD.

b) La generación de reportes deberá ser la herramienta de visualización en donde reposen los registros de conexiones, dispositivos y usuarios que han accedido a los recursos corporativos.

c) El monitoreo deberá estar parametrizado también en CISCO ISE para disponer de información en tiempo real que servirá al administrador de red para la realización de troubleshooting.

d) Las alarmas será otro aspecto a considerar dentro del esquema BYOD por medio de las cuales podrá proveer al administrador de red un recurso para prevenir algún tipo de evento malintencionado.

e) Tanto los mecanismos de reporteria, monitoreo y alarmas deberán estar configuradas de tal forma que se muestre parámetros más representativos como tiempo de conexión, dirección IP, dirección física, cantidad de dispositivos y usuarios conectados.

2.2.5 Segmentación de red.

a) Para que el esquema BYOD opere con un grado de seguridad aceptable, el administrador de red deberá parametrizar componentes como WLC y CISCO ISE de manera que se segmente el acceso físico a los recursos corporativos, es decir será pertinente proveer SSID's diferentes para el caso de la red inalámbrica, en donde funcionarios e invitados tengan la posibilidad de conectarse y la granularidad con la que se aplique la seguridad sea más eficiente.

b) La sintaxis para la red inalámbrica para funcionarios BYOD podría estar dispuesta de la siguiente manera: wbyod_funcionarios.

c) La sintaxis para la red inalámbrica para invitados BYOD podría estar dispuesta de la siguiente manera: wbyod_invitados.

d) La seguridad de la red inalámbrica es un factor que debe disponer de mecanismos seguros como EAP-TLS para asegurar la conexión.

3 Política de Identificación y Control de Acceso.

En la presente política se darán los lineamientos generales para que mediante mecanismos como antivirus, firewall y Wips se minimice el riesgo al que podría estar expuesta la infraestructura tecnológica, sus recursos y la información corporativa como su principal activo. El funcionario que adopte el esquema BYOD propuesto en la "Empresa Pública de Recaudación de Impuestos" deberá respetar los lineamientos estipulados a continuación.

3.1 Objetivo General

Definir los mecanismos que minimicen el riesgo de vulnerabilidades por parte de software malicioso o intentos de acceso no autorizado desde aquellos dispositivos que dentro de un esquema BYOD de la "Empresa Pública de Recaudación de Impuestos" hagan mal uso de sus privilegios.

3.2 Objetivos Específicos.

- Definir lineamientos para la utilización de un antivirus.
- Definir lineamientos BYOD de configuración de firewall.
- Definir lineamientos para monitorear amenazas en la red inalámbrica BYOD para funcionarios.

Muchas de las ventajas que un esquema BYOD provee para garantizar un control de riesgo a nivel de aplicaciones así como a nivel de privacidad de la información pueden ser gestionadas de manera eficiente y centralizada mediante un sistema MDM.

3.2.1 Antivirus

a) El esquema BYOD propuesto define el uso de un software antivirus que deberá ser obligatoriamente instalado en el dispositivo BYOD como requisito previo y deberá encontrarse al día en sus definiciones de virus con lo cual se garantizará la seguridad del dispositivo BYOD y al mismo tiempo el dispositivo cumplirá con políticas institucionales.

b) El antivirus propuesto será del mismo fabricante que actualmente está disponible en la "Empresa Pública de Recaudación de Impuestos".

3.2.2 Firewall

a) A nivel de firewall las configuraciones necesarias deberán estar enfocadas en filtrar el tráfico que entra y sale de los dispositivos BYOD legítimos.

b) Otra de las funciones que deberá incorporar será filtrado de tráfico de dispositivos BYOD según el tipo de conexión (wifi o celular), tipo de aplicación e incluso dirección IP.

c) Será responsabilidad del área o departamento de Seguridad Informática la configuración de las reglas y políticas dentro del firewall institucional con el afán de garantizar pruebas que certifiquen funcionamiento.

3.2.3 Wireless IPS.

a) Se deberá configurar adecuadamente los Access points que proveen servicio inalámbrico a los funcionarios de la institución de manera que se integre las funcionalidades de monitoreo mediante la tecnología WIPS.

b) El personal de Redes deberá validar la viabilidad de incorporar sensores WIPS a la infraestructura que provee servicio inalámbrico a los funcionarios si es que no los tuviese.

c) Se deberá contar con la capacidad de registrar todo tipo de eventos para detectar y detener amenazas que puedan darse desde posibles dispositivos BYOD comprometidos.

d) El almacenamiento y documentación de incidentes relacionados a posibles ataques será de utilidad para posibles investigaciones y posteriores acciones de índole civil o penal.

4 Política de Mantenimiento.

La presente política tiene por objetivo establecer lineamientos referentes a la revisión y mejora que se deberá realizar sobre la presente política en pro de gestionar el esquema BYOD propuesto en la "Empresa Pública de Recaudación de Impuestos".

4.1 Objetivo General

Establecer lineamientos que garanticen la revisión y mejora de la presente política para dotar de un documento actualizado constantemente y que a su vez facilite a los administradores de la infraestructura de red una visión amplia de las debilidades previas a adoptar un esquema BYOD dentro de la "Empresa Pública de Recaudación de Impuestos".

3.2 Objetivos Específicos.

- Definir el procedimiento para una revisión y mejora constante de la presente política.

3.2.1 Revisión y Mantenimiento de políticas.

a. Se deberá formar un equipo multidisciplinario compuesto por un miembro de las áreas de planificación, tecnología, jurídico, rrhh y seguridad institucional con el fin de realizar la revisión mensual de la presente política previa a ser implementada.

b. Esta revisión deberá cumplir con una periodicidad de al menos una revisión mensual durante diez meses.

c. El resultado de cada reunión deberá contemplar observaciones referentes a:

    a. Impacto a la seguridad institucional.

    b. Mejora a los mecanismos de conexión hacia la red inalámbrica.

c. Documentación legal a considerarse para la adopción de un esquema BYOD.

d. Inclusión de nuevas tecnologías para facilitar la administración de dispositivos móviles.

d. El mejoramiento deberá contemplar la inclusión de nuevas funcionalidades en favor de la institución considerando los siguientes aspectos:

   a. Generación de una política de protección de la información que incluya mecanismos como encriptación, limpieza de datos, respaldo de datos, bloqueo remoto, segmentación de información personal y corporativa, actualización de dispositivos.

   b. Análisis de factibilidad técnica y económica previo a la inclusión de un sistema MDM para facilitar funciones de administración.

GLOSARIO DE TÉRMINOS

On-Boarding: Término que define el proceso de registro y conexión de un dispositivo móvil al esquema BYOD.

Cisco ISE: Definida como Cisco Identity Services Engine es la plataforma que provee funcionalidades de seguridad y además facilita la provisión de funciones de BYOD.

VLAN: Se la define de manera lógica como una red de área local virtual que principalmente se utiliza para segmentar el tráfico de red.

ACL: Definida como una lista de control de acceso, se utiliza como mecanismo de seguridad para diferenciar los privilegios de acceso para un determinado objeto.

Troubleshooting: Es definido como un proceso lógico mediante el cual se puede determinar la causa y solución de un problema dentro del ámbito de las redes informáticas.

MDM: Mobile Device Management, es una plataforma que provee capacidad de asegurar, monitorear y gestionar los dispositivos móviles conectados en un esquema BYOD.