31/05/2019

COD: A205

INFORMÁTICA / TELECOMUNICACIONES

PRIMER EJERCICIO
SEGUNDA PRUEBA

Tiempo máximo: 100 minutos
Preguntas: 100.

MODELO / EREDUA:	**A**

- No abra el cuadernillo hasta que se le indique.
- Marque en la hoja de respuestas el modelo que le haya correspondido.
- A la finalización de la prueba recoja este cuadernillo, la copia amarilla de su hoja de respuestas y la hoja de instrucciones.
- Recuerde:
  - Aciertos: 1,00
  - Errores, nulos, dobles o blancos: no descuentan.
- La ausencia de marca o la marca incorrecta en el modelo invalida la prueba.
- No se entregarán nuevas hojas de respuesta en los últimos 5 minutos del ejercicio.
- Cuando finalice levante la mano y el personal de la organización recogerá la hoja de color blanco
- No se recogen exámenes individualmente en los últimos 3 minutos del ejercicio. Si ha finalizado permanezca en su sitio en silencio hasta la recogida final.

Gracias por su colaboración

1.- El cableado UTP de pares trenzados se clasifica en diferentes niveles o categorías. El que mayor velocidad soporta se denomina
a) UTP categoría 6
b) UTP categoría 1
c) UTP categoría 5e
d) UTP categoría 4

2.- En una red LAN, si los datos pueden ir en los dos sentidos, pero no a la vez, la comunicación se denomina:
a) Full Duplex
b) Half Duplex
c) Simplex
d) Complex

3.- La red que conecta el router de una empresa/domicilio con el proveedor de servicios de internet (ISP) se denomina:
a) LAN
b) SAN
c) WAN
d) PAN

4.- Significado de las siglas SIP:
a) Protocolo de transferencia de hipertexto
b) Protocolo de transferencia de mensajes
c) Protocolo de inicio de sesión
d) Protocolo de inicio de servicio

5.- Tres elementos fundamentales de la arquitectura de red que define el estándar de telefonía IP
a) Terminales, routers y switches
b) Terminales, gatekeepers y gateways
c) Routers, gatekeepers y switches
d) Routers, switches y gateways

6.- ¿Cual de los siguientes NO es un protocolo de VoIP?
a) Skype
b) NTP
c) IAX
d) SCCP

7.- Protocolo que NO se utiliza para establecer VPNs
a) IPSEC
b) L2TP
c) XMPP
d) PPTP

8.- El protocolo L2TP es heredero de los protocolos
a) PPTP y SSH
b) PPTP y L2F
c) IPSEC y SSL/TLS
d) IPSEC y PPTP

9.- Puerto TCP asignado por defecto al protocolo SSH
a) 21
b) 22
c) 80
d) 8080

10.- Norma IEEE en la que se estandariza el protocolo STP
a) 802.1AQ
b) 802.1D
c) 802.1X
d) 802.1W

11.- Principal inconveniente del protocolo STP
a) Sólo se puede aplicar con switches del mismo fabricante
b) Es poco seguro
c) Tiempo que tarda en converger
d) Consume mucha CPU

12.- En RSTP (Rapid STP), NO existe un estado de un puerto denominado
a) Learning
b) Inspecting
c) Forwarding
d) Discarding

13.- Para configurar una VLAN de nivel 1
a) Hay que especificar los puertos del switch que pertenecen a esa VLAN
b) Se asignan equipos a la VLAN en función de su dirección MAC
c) La VLAN queda determinada por el contenido del campo “tipo de protocolo” de la trama MAC
d) Se utiliza la cabecera de nivel 3 para mapear la VLAN a la que pertenece el equipo

14.- El protocolo de etiquetado de VLAN es el estándar:
a) 802.AD
b) 802.1Q
c) 802.1W
d) 802.1X

15.- Indique cual NO es un modo de operación del protocolo VTP (VLAN Trunking Protocol)
a) Servidor
b) Controlador
c) Cliente
d) Transparente

16.- Para establecer un trunking VLAN en ambos puertos extremos
a) Debe estar configurada la misma VLAN nativa
b) No debe existir previamente ninguna VLAN
c) Se debe configurar FullDuplex
d) Los equipos tienen que ser del mismo fabricante

17.- Para que un puerto de un switch pueda pertenecer a más de una VLAN hay que definirlo como
a) Modo access
b) Modo trunk
c) Modo FullDuplex
d) No hay que indicar nada, es automático

18.- Cual de los siguientes NO es un objetivo de NAC (Control de Acceso a la Red):
a) Mitigar ataques de día cero
b) Reforzar las políticas de acceso
c) La administración del acceso e identidad
d) La gestión del ancho de banda de las conexiones

19.- Para que un usuario legítimo, sin derecho de acceso directo a internet pueda hacerlo, el sistema NAC se lo proporciona con:
a) Portales cautivos
b) Conexiones alternativas inalámbricas
c) Asignación de direcciones IPv4 por DHCP
d) Asignación de direcciones IPv6 asociadas a la MAC

20.- Servidor DNS OpenSource más utilizado:
a) apache
b) ntp
c) bind
d) openldap

21.-Entre los tipos de servidores DNS, según la función que desempeñan, NO figura el tipo de servidor
a) Primario
b) Local
c) Secundario
d) Global

22.- Tipo de registro DNS que NO existe
a) SOA
b) NS
c) AA
d) ANY

23.- Dominio especial utilizado en la resolución inversa DNS de direcciones IPv4:
a) ipv4.arpa
b) internet.arpa
c) in-addr.arpa
d) i-net.arpa

24.- PDU utilizada por un cliente DHCP para solicitar una dirección IPv4 a un servidor
a) DHCPACK
b) DHCPDISCOVER
c) DHCPREQUEST
d) DHCPOFFER

25.- DHPC, entre los métodos de asignación de direcciones IPv4, NO tiene uno denominado
a) Asignación manual o estática
b) Asignación automática
c) Asignación dinámica
d) Asignación explícita

26.- DHCPv6 funciona sobre el protocolo de transporte
a) TCP
b) NTP
c) UDP
d) FTP

27.- Los sistemas de triple factor de seguridad, además de pedir nombre de usuario y contraseña, habitualmente…
a) Solicitan responder a una pregunta personal
b) Utilizan un sistema de reconocimiento biométrico
c) Solicitan firmar un documento de confidencialidad
d) Utilizan CAPTCHA

28.- El método más eficaz para securizar un servicio de red es
a) Utilizar un nombre poco significativo
b) Cambiar el puerto TCP o UDP por defecto
c) No publicarlo en el DNS
d) Utilizar certificados SSL

29.- Para detener posibles ataques, es conveniente integrar los sistemas IDS (Intrusion Detection Systems) con
a) El sistema antivirus corporativo
b) El firewall de la red
c) El switch de acceso de usuarios
d) El sistema de autenticación de la organización

30.- Cual de las siguientes NO es una forma de detección de tráfico malicioso en los IPS (Intrusion Prevention Systems)
a) Detección basada en protocolos
b) Detección basada en firmas
c) Detección basada en políticas
d) Detección basada en anomalías

31.- Señale el mecanismo más seguro utilizando por los sistemas antivirus
a) Firma digital
b) Detección heurística
c) Detección por comportamiento
d) Detección por sandboxing

32.- Sistema o tecnología que puede comprometer la “neutralidad de la red”
a) Firewall
b) IDS (Intrusion Detection Systems)
c) DPI (Deep Packet Inspection)
d) IPS (Intrusion Prevention Systems)

33.- Una red WiFi 802.11 que opera en la frecuencia de 2,4GHz tiene un máximo de
a) 10 canales
b) 14 canales
c) 16 canales
d) 20 canales

34.- El método de seguridad que utiliza AES (Advanced Encryption Standard) en redes WiFi es
a) Wired Equivalent Privacy (WEP)
b) Wi-Fi Protected Access (WPA)
c) Wi-Fi Protected Access II (WPA2)
d) Wi-Fi Protected Setup (WPS)

35.- Velocidad teórica máxima de una red WiFi 802.11g
a) 11 Mbps
b) 54 Mbps
c) 100 Mbps
d) 600 Mps

36.- La norma EIA/TIA 568A para cableado horizontal UTP se aplica a una topología de red en:
a) Bus
b) Anillo
c) Estrella
d) Red mallada

37.- Radio mínimo de curvatura en condiciones de no tensión, recomendado para cableado UTP
a) Tres veces el diámetro del cable
b) Cuatro veces el diámetro del cable
c) Cinco veces el diámetro del cable
d) Seis veces el diámetro del cable

38.- Radios mínimos de curvatura en condiciones de no tensión, recomendados para mangueras de Fibra Optica
a) 50 centímetros de radio en todos los casos
b) 5 a 10 veces el diámetro de la manguera
c) 10 a 20 veces el diámetro de la manguera
d) 20 a 40 veces el diámetro de la manguera

39.- La tecnología GPON de fibra óptica se emplea para
a) Redes MAN
b) Redes WAN
c) Conexión entre nodos de comunicaciones
d) Conexión de usuarios (FTTH)

40.- La tecnología óptica WDM se utiliza principalmente en:
a) Conexiones por fibra multimodo de equipos de usuario
b) Conexiones por fibra óptica monomodo entre servidores
c) Conexiones entre routers, por fibra óptica de cualquier tipo
d) Redes ópticas con fibra monomodo

41.- Las redes FDDI utilizan
a) Radioenlaces
b) Par trenzado UTP
c) Fibra óptica
d) Cable coaxial (CATV)

42.- En un radioenlace fijo de tipo dúplex, las estaciones repetidoras activas:
a) Demodulan la señal
b) Bajan la señal a una frecuencia intermedia para amplificarla
c) Actúan como espejos que reflejan la señal
d) Reencaminan las tramas en una red mallada

43.- Las “pérdidas en la alimentación” que sufre la señal en los radioenlaces se deban a
a) El tipo de suministro de energía eléctrica, continua o alterna
b) La altura de la torre o del edificio en donde se coloca la antena
c) La frecuencia utilizada
d) El ancho de banda del canal

44.- Señale la respuesta CORRECTA . Los dos protocolos básicos en VoIp son
a) RTP y SNMP
b) TCP y HTTP
c) UDP y SIP
d) SNMP y H323

45.-Señale la respuesta CORRECTA . De cuantas fases se compone la configuracion-implementacion de un tunel IPSEC por método IKE ?
a) 1
b) 4
c) 3
d) 2

46.-Señale la respuesta CORRECTA. Un terminador SSL puede servir para permitir el acceso a la ejecución de servicios desde Internet?

a) Sólo si son servicios no esenciales.
b) Solo si las URL´s a las que se acceda no tienen derivaciones a otras URL´s.
c) Solo a usuarios autorizados a nivel de terminador de túneles .
d) Siempre que los usuarios autorizados por el terminador de túneles tengan permisos para las aplicaciones de los servicios expuestos

47.- Señale la respuesta CORRECTA. La fase II de un tunel IPSEC con negociación IKE se refiere a :

a) La negociación de una Asociación de Seguridad entre los extremos del túnel
b) El establecimiento de un canal seguro entre los extremos del túnel
c) La identificación de los extremos del túnel por sus claves
d) Tener la certeza de que el algoritmo Diffie-Hellman funciona adecuadamente.

48.- Señale la respuesta CORRECTA . En la configuracion IPSEC de un túnel LAN to LAN se configura la gestión del tráfico. Concretamente de :

a) Sólo de las redes locales desde las que se accede
b) Sólo de las redes remotas a las que se accede
c) Las redes locales y las remotas
d) Ninguna red. Las redes se definen en el Firewall de perímetro

49.- Señale la respuesta CORRECTA . Prtocolo HSRP: Los routers que ejecutan HSRP se comunican de esta funcionalidad a través de:

a) Paquetes HSRP Hello
b) Paquetes HSRP Ack
c) Paquetes ICMP
d) Paquetes Sync

50.- Señale la respuesta CORRECTA. La dirección IP virtual que se mostrará a la red en un grupo VRRP estará asociada a:

a) El router que actue como master
b) Al grupo de routers que propongan la métrica mas corta.
c) Al router que este activo con mayor antigüedad
d) Al router que reciba más tráfico inter-LAN

51- Señale la respuesta CORRECTA . HSRP y VRRP pueden estar configurados en el mismo router

a) Si se asocian al mismo interface
b) Nunca
c) Si están asociados a diferentes interfaces
d) Siempre

52.- Señale la respuesta CORRECTA. Los protocolos de enrutamiento dinámico se clasifican en:

a) Vector distancia y Estado de Enlace
b) Vector distancia y Hop-counting
c) Reliability Status y Estado de Enlace
d) De Gateway Interior y de Gateway de Frontera

53- Señale la respuesta CORRECTA. Una ruta dinámica se construye

a) Por la información que se intercambian los protocolos de enrutamiento
b) Automáticamente cuando las rutas estáticas fallan.
c) Cuando la red es pequeña
d) No hay rutas redundantes

54.- Señale la respuesta CORRECTA. La tecnología Crossbar en los Nexus se refiere a:
a) Al tráfico que va por el backplane interno de los Nexus, que interconectan los módulos IO y las supervisoras
b) Al tráfico entre la memoria Flash de arranque y la Supervisora.
c) Al intercambio de señales de control entre Supervisora y Memoria.
d) Al orden de transmisión de los paquetes almacenados.

55.- Señale la respuesta CORRECTA. En referencia a la MIB: Management Information Base
a) MIB II es un subconjunto de MIB I
b) Esta compuesta de direcciones IP de los dispositivos en la red
c) Las MIBs son estáticas en el tiempo
d) Define variables utilizadas por el protocolo SNMP

56.- Señale la respuesta CORRECTA . Herramienta TCPDUMP.
a) Es una herramienta sólo para Windows
b) Es una buena herramienta para análisis de tráfico de red en Linux y UNIX
c) El comando: # tcpdump -i eth0 captura el tráfico de entrada del interfaz eth0
d) El comando: # tcpdump 'dst 192.168.1.100 and (port http or https)' captura el tráfico de origen 192.168.1.100 de los puertos http o https

57.- Señale la respuesta CORRECTA . Al ejecutar el comando de SYSLOG-NG: service syslog-ng restart
a) Rearranca syslog-ng y hace que los cambios realizados en su configuración se activen
b) Rearranca syslog-ng con una versión estable almacenada en el fichero de cambios de la Flash.
c) Sólo permite arrancar syslog-ng desde un servidor remoto.
d) Arranca syslog-ng para iniciar su configuración en modo manual.

58.- Señale la respuesta CORRECTA: El protocolo SNMP
a) Es un protocolo de capa Transporte que posibiita el intercambio de datos de administración entre dispositivos de red.
b) Es un protocolo de capa Aplicación que posibilita el intercambio de datos de administración entre dispositivos de red .
c) Es un protocolo de capa Red que permite el intercambio de datos de gestión entre dispositivos de red.
d) Es un protocolo de capa Transporte que permite el almacenamiento y procesado de datos de administración entre dispositivos de red.

59.- Señale la respuesta CORRECTA. SNMP funciona en los siguientes modos:
a) Proactive y Supervisor
b) Mirror y Promiscuo
c) Basic y Advanced
d) Polling y Traps

60.- Señale la respuesta CORRECTA. La utilidad Sand-Box en Fortinet , denominada Fortisandbox
a) No es una herramienta eficaz para la prevencion de amenazas de Zero Day
b) Dota a los usuarios de una avanzada herramienta de APT (Amenazas Persistentes Avanzadas)
c) No es capaz de detectar un ataque de Crypto Locker
d) Solo se puede implementar en combinación con la plataforma FortiMail

61.- Señale la respuesta CORRECTA. Administra el FortiManager al FortiAnalyzer?
a) Es posible pero no es la implementación recomendada.
b) No
c) Solo para determinados flujos de trabajo y en en servicio FortiCloud.
d) Si. Es la implementación recomendada.

62.- Señale la respuesta CORRECTA. La utilidad de WEB Filtering en entorno Fortinet:
a) No se pueden bloquear páginas Web específicas, solo categorías.
b) Su objetivo es la detección de contenidos maliciosos
c) Sólo se puede configurar en entorno GUI
d) El URL Filtering es una parte de la función de Web Filtering

63.- Señale la respuesta CORRECTA . La utilidad IPS :
a) Solo se puede implementar como un dispositivo software.
b) Es sólo un sistema de detección de intrusiones.
c) Permite bloquear tráfico malicioso.
d) CheckPoint no lo tiene en su portfolio de productos.

64.- Señale la respuesta CORRECTA. La utilidad Sand-Box en Fortinet , denominada Fortisandbox
a) No puede implementarse en la Nube. Solo permite implementaciones en appliance y en máquina virtuales
b) Solo puede funcionar integrado con Fortimail
c) Funciona en modo nativo con Smart Event para la gestión de eventos.
d) Permite crear una red simulada de archivos explorados a los que acceder en un entorno de red cerrado

65.- Señale la respuesta CORRECTA . La utilidad IPS :
a) Es capaz de inspeccionar el tráfico HTTPS en determinadas implementaciones
b) Inspecciona el tráfico encriptado por defecto.
c) Avisa al usuario final siempre que no permite el paso de algún tráfico que le afecte.
d) En un IPS, el tráfico HTTP necesita ser descifrado para ser inspeccionado

66.- Señale la respuesta CORRECTA. Que significan las siglas FWAAS o FAAS
a) Forwarding and Act Service
b) Forwarding as a Service
c) Firewall as a Service
d) Frame welding as a Service

67.- Señale la respuesta CORRECTA. El IPS de Fortinet:
a) La incorpora Fortinet en su solución NGFW (Next Generation Firewall)
b) Necesita plugins específicos para integrarse con FortiAnalyzer
c) Fue un desarrollo externo adquirido por Fortinet en 2013
d) Permite integración con otros partners: FireMon, Gigamon….

68.- Señale la respuesta CORRECTA. Tecnología Mesh en WIFI.
a) Esta basada en dos controladores en HA y AP´s con MIMO.
b) Su objetivo es componer redes WIFI redundantes con múltiples SSID.
c) Los portales son diferentes en función de la estación base o repetidor/AP al que se vincula un usuario.
d) El mecanismo de autenticación y autorización es el mismo para toda la red Mesh.

69.- Señale la respuesta CORRECTA. La herramienta FortiAnalyzer de Fortinet.
a) Permite un cierto análisis forense
b) El procedimiento de copia de respaldo de la BBDD de FortiAnalyzer precisa de autorización del FortiManager
c) Las tramas de determinados modelos antiguos de Firewall Fortinet deben ser desencriptadas con un hash propio de Fortigate para poder ser gestionadas por el FortiAnalyzer
d) El alto volumen de datos manejado hace que no sea una herramienta adecuada para detección de amenazas sino sólo para análisis de logs

70.- Señale la respuesta CORRECTA. Un WAF es:
a) Un Firewall de Aplicacion Web que se instala en la red interna solamente.
b) Un firewall ubicado entre un cliente Web y un servidor Web que analiza las comunicaciones en la capa de transporte.
c) Un firewall de capa 7 con un blade IPS.
d) Un Firewall de capa 7 para aplicaciones Web

71- Señale la respuesta CORRECTA. El módulo Clear Pass Guest
a) Permite gestionar la seguridad a nivel MDM de dispositivos móviles corporativos
b) Permite la provisión de invitados mediante un portal cautivo
c) Perite el acceso seguro sólo a redes WIFI
d) El login va en texto plano

72.- Señale la respuesta CORRECTA. Clear Pass:
a) Siempre utiliza CA´s externas.
b) No es compatible con / soporta LDAP, sólo con AD.
c) Permite autenticación por MAC
d) No dispone de herramientas de report.

73.- Señale la respuesta CORRECTA. La herramienta AIRWAVE
a) Es un sistema de gestión sólo de redes WIFI, haciendo especial énfasis en la gestión de canales radio.
b) Al ser un producto de HPE-Aruba, sólo permite la gestión de dispositivos Aruba.
c) Permite un mapeo de la red, incluso a nivel de RF
d) Los dispositivos deben ser introducidos (identificados) manualmente en la BBDD de Airwave.

74.- Cual de estos conceptos NO se refiere a la gestión, detección y prevención de ciber amenazas?
a) Cumplimiento del ENS
b) Analytics Powered Security
c) Next Generation Firewall
d) Open Shortest Path First

75.- Señale el enunciado FALSO. Acerca de WIFI:
a) El estándar 802.11b usa la banda de 2,4 Ghz
b) El estándar 802.11ac utiliza una tecnología que focaliza señales radio y puede atravesar paredes.
c) El estándar 802.11ac usa bandas duales, permitiendo conexiones a 2,4 y 5 Ghz.
d) El estándar 802.11a usa la banda de 5 Ghz.

76.- Señale el enunciado FALSO. Acerca de WIFI:
a) Se puede montar una arquitectura con controladoras en Alta Disponibilidad
b) Una red WIFI es el único método de control de seguridad de los dispositivos móviles
c) Un portal cautivo y un RADIUS son componentes del sistema de acceso y autenticación
d) Los AP´s de un sistema WIFI deben ser compatibles con la/las controladoras.

77.- Señale el enunciado FALSO. Acerca del Blade de Software Anti-Spam y Email Security de CheckPoint
a) Lleva embebido un IPS para protección correo contra ataques de denegación de servicio : Denial of Service (DoS) - buffer over-flow attacks .
b) Incluye protección anti virus basados tanto en zero-day como en firmas .
c) Los administradores pueden crear listas de direcciones IP o dominios, bien para bloquearlos o para permitirlos.
d) Necesita la herramienta de gestión Smart Event para su configuración

78.- Señale el enunciado FALSO. El URL Filtering
a) Permite la creación de categorías o perfiles de acceso a Internet.
b) Dota de una herramienta de control de accesos a Internet al administrador de red
c) Puede reducir los incidentes de malware bloqueando el acceso a páginas conocidas de contenido malicioso.
d) Es una herramienta sólo de Operadoras "As a Service"

79.- Señale el enunciado FALSO. Los Firewalls:
a) Puede hacer labores de Proxy: firewall proxy
b) Un "Stateful Inspection Firewall" permite el bloqueo de tráfico según criterios basados en estado puerto y protocolo
c) Es un dispositivo sólo Software
d) Han evolucionado para atender la nuevas amenazas de malware o de capa 7.

80.- Señale el enunciado FALSO. La utility IPS en los firewall Fortinet
a) Viene incorporada en su solucion Next Generation Firewall.
b) Hace falta activarlo en un blade específico
c) Inspecciona el contenido de las comunicaciones .
d) Se puede administrar conjuntamente a los firewalls de Fortinet.

81- Señale el enunciado FALSO. El módulo Policy Manager de la herramienta Clear Pass de Aruba :
a) Soporta múltiples fuentes de autenticación / autorización
b) Permite establecer políticas por tipo de dispositivo
c) Necesita un servidor TACACS externo
d) Ayuda a establecer políticas BYOD

82.- Señale el enunciado FALSO. Los controladores WIFI de ARUBA:
a) Permiten la gestión de varios AP¨s simultaneamente, según modelos.
b) Pueden estar virtualizados.
c) Permiten el acceso de usuarios concurrentes ilimitados.
d) Un Instant AP no necesita Controlador para funcionar en una red empresarial.

83.- Señale el enunciado FALSO. Clear Pass:
a) Permite gestión BYOD sólo de dispositivos HPE-Aruba
b) Permite la creación de portales de invitados personalizados.
c) Facilita el auto registro de usuarios en una red.
d) Permite el auto registro por credenciales de Facebook.

84.- Señale el enunciado FALSO. La herramienta AIRWAVE
a) Con su función AppRF proporciona visibilidad profunda de aplicaciones comunes y del tráfico web en la red.
b) El módulo complementario Aruba Clarity analiza proactivamente la calidad de experiencia de los usuarios finales.
c) AirWave RAPIDS™ Rogue Detection detecta y localiza AP´s y cllientes no autorizados
d) VisualRF es una herramienta de generación de reports de seguridad, asociado a herramientas de "Pentesting" propias y de terceros.

85.- Señale el enunciado FALSO. Un túnel IPSEC LAN to LAN sirve para :
a) Conectar dos sedes.
b) Permitir el acceso de usuarios a una red protegida.
c) Proteger una LAN de accesos remotos no autorizados.
d) Mitigar posibles intrusiones desde una red remota

86.- Señale el enunciado FALSO. En Nexus, la tecnología FEX (Fabric Extender) :
a) Se refiere a una extensión del fabric de conmutación a dispositivos de frontera (EDGE) (switches, routers… puntos de acceso a la red de usuario.
b) Permite una gestión completa como parte del "switch padre"
c) Solo puede configurarse con STP (Spanning Tree Protocol) para el control de caminos redundantes.
d) FEX permite el uso de ACL´s que estén disponibles en el "switch padre"

87.- Señale el enunciado FALSO. Sobre el modo de funcionamiento de RADIUS
a) Utiliza TCP como protocolo de transporte
b) Un servidor RADIUS puede funcionar como cliente proxy para otros servidores RADIUS
c) El cliente envia el nombre del usuario y la contraseña encriptada al servidor RADIUS
d) Los procesos de Autenticación y Autorización se complementan con el de Contabilización en una arquitectura de AAA con RADIUS

88.- Señale el enunciado FALSO. En un servidor RADIUS
a) El protocolo RADIUS es Cliente-Servidor
b) Suele haber una Base de Datos de Usuarios
c) Solo soporta un método de autenticación de usuarios: el PPP
d) En general, RADIUS se considera un servicio sin conexión

89.- Señale el enunciado FALSO. En un entorno WIFI, el uso de RADIUS
a) Puede suponer una alternativa a utilizar WPA con clave fija en entornos de pocos usuarios.
b) Puede ir controlado por el Active Directory
c) Va asociado con una asignación fija de direccionamiento IP
d) Puede funcionar con una Base de Datos de usuarios

90.- Señale el enunciado FALSO. El sistema de monitorización NAGIOS
a) Permite la monitorización remota a través de diversos tipos de túnel.
b) Permite la monitorizacion de diversos recursos de equipos hardware.
c) Permite la prevención y mitigación de diversos tipos de malware.
d) Permite el diseño simple de plugins

91.- Señale el enunciado FALSO. . SYSLOG-NG
a) Puede funcionar con una gestión centralizada de logs
b) Puede funcionar como aplicación stand-alone
c) Es un buen complemento de soluciones SIEM
d) No permite utilizar TCP

92.- Señale el enunciado FALSO. ¿Qué ocurre cuando el nodo Maestro cae en una configuración de routers con VRRP?:
a) Uno de los nodos Esclavo asume el rol de Maestro.
b) En el nuevo router deben ser configuradas manualmente las rutas dinámicas.
c) La IP y MAC virtual son las mismas para cualquier router que asuma el rol de Maestro.
d) No tenemos que cambiar las rutas de destino hacia este router desde otras redes.

93.- Señale el enunciado FALSO. Herramienta WIRESHARK
a) Un port mirroring es una buena técnica de usar la herramienta Wireshark
b) Wireshark se puede uar en modo bridge - Man in the middle ,con dos tarjetas de red.
c) Wireshark sirve para mitigar un ataque de ARP SPOOF
d) Wireshark sirve para averiguar si se está produciendo un ataque de ARP SPOOF

94.- Señale el enunciado FALSO. INTERMAPPER
a) Se puede configurar cuando y como detectar nuevos dispositivos de red .
b) Se pueden configurar eventos de red y hacer una supervisión proactiva.
c) Es capaz de identificar amenazas del tipo DDoS en base a triggers de tráfico
d) Se puede montar sobre plataformas MAC, LINUX y Windows.

95.- Señale el enunciado FALSO. SYSLOG-NG :
a) Se pueden realizar extensiones de Syslog-ng en Python o C
b) Se pueden enviar y almacenar los datos en diversas BBDD
c) Es una herramienta desarrollada y licenciada por Microsoft
d) Permite el transporte de mensajes encriptados

96.- Señale el enunciado FALSO. Acerca de la herramienta/ suite NAGIOS:
a) Se pueden monitorizar servicios de Microsoft Windows.
b) Lleva embebido una potente herramienta de monitorización, análisis y gestión de logs.
c) Su herramienta de análisis de red no permite ser proactivo en la resolución de posibles incidencias debido a los retrasos en la recepción de traps en redes complejas.
d) Tiene una arquitectura expandible , pudiendo, con múltiples API´s integrar productos / aplicaciones de terceros.

97.- Señale el enunciado FALSO. Acerca del gestor de red NTERMAPPER:
a) Solo permite un nivel de mapas, sin poder crear submapas
b) Es posible integrar con Google Maps o Earth
c) Los reports disponibles son variados y customizables
d) Permite visibilidad de conexiones en Capa 2 y 3

98.- Señale el enunciado FALSO. En el análisis de paquetes usando la herramienta WIRESHARK
a) Podemos distinguir básicamente entre filtros de captura y filtros de visualización.
b) Podemos distinguir básicamente entre filtros simples y booleanos
c) Podemos extraer el flujo de datos establecido en una sesión TCP.
d) Existe una funcionalidad denominada EXPERT INFOS.

99.- Señale el enunciado FALSO. La utilidad Sand-Box en CheckPoint, denominada SandBlast; :
a) Permite ejecutar o analizar ficheros en un entorno controlado
b) Permite analizar un amplio rango de documentos de los más habituales
c) Permite integrarse con herramientas de análisis forense
d) Solo se puede implementar en soluciones basadas en Appliances

100.- Señale el enunciado FALSO. El producto Smart Event de CheckPoint?
a) Permite una visibilidad completa de los riesgos de seguridad del entorno CheckPoint.
b) Permite un cierto análisis forense en tiempo real.
c) Lleva implementadas “de serie” una serie de políticas suficientes para detectar un gran número de eventos de seguridad.
d) Es capaz de interpretar de manera nativa eventos de seguridad de firewalls Fortinet.

Ayuntamiento de Vitoria-Gasteiz
Vitoria-Gasteizko Udala

OPE2017-18
A205 31/05/2019
1. Ariketa- 2. Proba / 1. Ejercicio 2ª. Prueba
A/D–B Ereduko Behin-behineko Txantiloia – Plantilla provisional. Modelo A/D Y B

Nº	A
1	A
2	B
3	C
4	C
5	B
6	B
7	C
8	B
9	B
10	B
11	C
12	B
13	A
14	B
15	B
16	A
17	B
18	D
19	A
20	C
21	D
22	C
23	C
24	C
25	D
26	C

Nº	A
27	B
28	D
29	B
30	A
31	D
32	C
33	B
34	C
35	B
36	C
37	B
38	C
39	D
40	D
41	C
42	B
43	B
44	C
45	D
46	D
47	A
48	C
49	A
50	A
51	C
52	A

Nº	A
53	A
54	A
55	D
56	B
57	A
58	B
59	D
60	B
61	D
62	D
63	C
64	D
65	A
66	C
67	A
68	D
69	A
70	D
71	B
72	C
73	C
74	D
75	A
76	B
77	D
78	D

85

Nº	A
79	C
80	B
81	C
82	C
83	A
84	D
85	D
86	C
87	A
88	C
89	C
90	C
91	D
92	B
93	C
94	C
95	C
96	C
97	A
98	B
99	D
100	D

25/09/2019

A205. INFORMATICA-TELECOMUNICACIONES

SEGUNDO EJERCICIO
Tiempo máximo: 140 minutos
Pd Max: 1.000 puntos
Puntuación prueba: 30 puntos

No abra el cuadernillo hasta que se le indique y lea atentamente las instrucciones de esta portada.

- **Móviles apagados** y, al igual que los relojes, pulseras de actividad y similares, retirados de la mesa. Botellas de agua, estuches y similares pueden tenerse accesibles pero no sobre la mesa.
- Si no hay reloj en la sala, se informará por voz del tiempo que falta para la realizar la prueba: 60-30-15-10-5 y último minuto.
- Sobre la mesa exclusivamente cuadernillo de preguntas, hoja de identificación personal, DNI y bolígrafo (azul o negro). Se permite la utilización de rotuladores de color y de TIPEX® o similares.
- Utilice en su ejercicio un tipo **de letra que permita su lectura** por el Tribunal.
- Si se le ha facilitado una **hoja de identificación** con una CLAVE rellénela con su DNI, nombre, apellidos y código/denominación de la prueba.
- **Escriba la CLAVE en las hojas de respuesta** que vaya a utilizar. NO escriba su nombre, DNI o firme la prueba ya que es causa de NO CORRECCIÓN. Utilice ambas caras del folio. Numere folios, no páginas.
- La Hoja de Identificación se recogerá transcurridos los primeros minutos de la prueba.
- Si desea un **certificado de asistencia** solicítelo en el momento en el que se le realice el control de presencia.
- Las respuestas deberán ser concretas y precisas. La corrección se realizará conforme a criterios predeterminados. La valoración máxima de cada pregunta, en el caso de ser diferentes, viene señalada en el enunciado de la misma.
- Si ha finalizado antes de tiempo levante la mano para que se le recoja la hoja de respuestas. No se recogen exámenes individualmente en los últimos 3 minutos del ejercicio y si ha finalizado en este plazo permanezca en su sitio, en silencio, hasta la recogida final,
- No olvide indicar en todas sus hojas de respuestas:
  - **Código OPE (A205)**
  - **Clave** identificación
  - **Caso/supuesto. (Iniciar cada supuesto en una hoja nueva**)
  - **Número de hoja** / **total** de hojas utilizadas
- Ejemplo CABECERA:

COPE Zuzentzeko kodea / Clave de corrección	Kasua-Ustezkoa / Caso-Supuesto	Ariketaren orria - Hoja / Guztira - Total hojas prueba
A-205	OP9999ZZZZZ	1	1 / 4
A-205	OP9999ZZZZZ	1	2 / 4
A-205	OP9999ZZZZZ	2	3 / 4
A-205	OP9999ZZZZZ	2	4 / 4

SUPUESTO 1: PROYECTO DE MIGRACION DE UNA RED DE COMUNICACIONES ENRUTADA (LAYER 3) A LAYER 2 (600 puntos)

En el marco de una organización compleja como el Ayuntamiento de Vitoria-Gasteiz (en adelante AVG), tenemos una arquitectura de conmutación en varios niveles (backbone, acceso) con dos routers en HSRP para obtener la alta disponibilidad en el routing. El routing, en una organización, permite la conectividad Inter-redes.

Todas las redes del AVG son IP´s de clase C, con default gateways a un cluster de routers que actúan en modo activo-activo.

PLANTEAMIENTO DEL EJERCICIO

Debido a diversos factores tales como:

- Dispersión geográfica de los diferentes servicios que componen el AVG
- Mejora del rendimiento de los trabajadores al poder desempeñar su trabajo en varias sedes.
- Flexibilidad de las instalaciones.
- Implantación masiva de tecnología Voz Ip.
- Futuro IoT inminente

Se plantea un cambio de arquitectura de conmutación de la Red Corporativa de Datos del Ayuntamiento de Vitoria-Gasteiz de la actual a capa 3 a una más flexible a capa 2 basado en VLAN´s. Permitirá dotar a la red Corporativa del AVG de una gran flexibilidad en sus implantaciones, obteniendo las **siguientes mejoras:**

- Conexión de redes lógicas en cualquier punto de la red Corporativa.
- Dotar de calidad de servicio – QOS- a las comunicaciones.
- Redes disgregadas multisede.
- Creación y mantenimiento sencillo.
- Seguridad embebida si la arquitectura así lo contempla.

ARQUITECTURA ACTUAL

NODO-1, NODO-2 y NODO-3 son los nodos principales de una red de backbone de la cual cuelgan nodos secundarios, conformando entre todas la estructura de Red Corporativa del Ayuntamiento de Vitoria-Gasteiz.

Estos NODOS están conectados al Cluster de Routers (2) que funcionan entre si en HSRP.

Conectados a la Red Corporativa, pero ajenas a ésta (se separan por Firewalls o routers, hay conexiones a Redes Externas (proveedores, otras organizaciones…).

Por otro lado, y de manera análoga, existe una barrera perimetral de protección hacia Internet donde también tenemos conexiones VPN, SSL´s, la propia conexión a Internet…

La arquitectura actual tiene además las siguientes características:

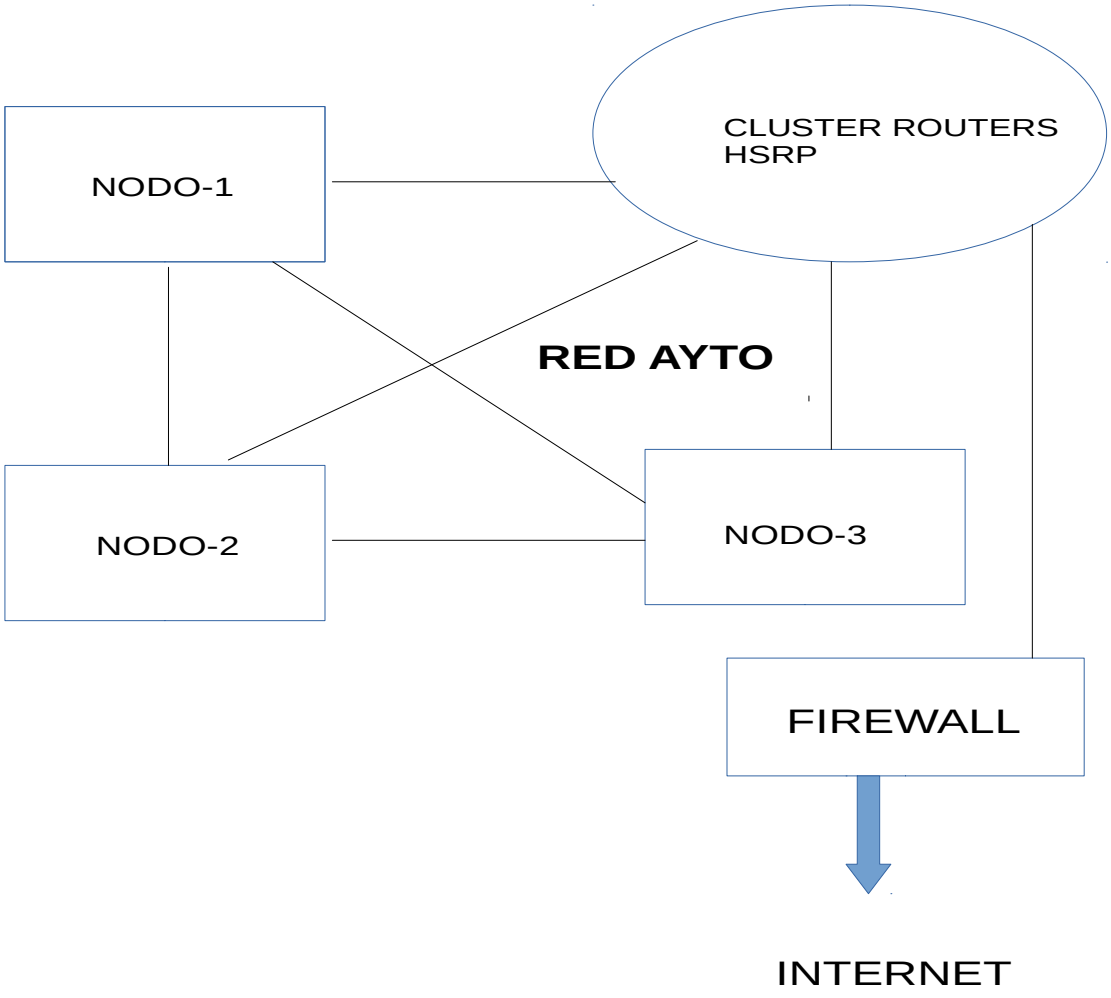
- Todos los nodos que forman parte de la red AYTO están unidos entre sí a nivel 3, incluyendo los Conmutadores de BackBone Cisco . Esto quiere decir que las redes definidas en cada nodo o rama está aislada a ese nodo o rama.
- La manera de proporcionar alta disponibilidad entre los distintos caminos que enlazan los nodos entre sí es mediante un proceso de routing dinámico OSPF.

La principal limitación de esta arquitectura es que las subredes definidas en cada uno de los nodos están confinadas a dichos nodos o ramas. No es posible extender alguna de estas subredes a más de un nodo o rama, impidiendo poder extender las subredes.

La **RED AYTO** incluye todas las subredes de trabajo de los trabajadores del Ayuntamiento de Vitoria-Gasteiz, las redes de servidores (en los CPD´s). Estas subredes se distribuyen entre 3 nodos o ramas:

- NODO-1
- NODO-2
- NODO-3

Además de las subredes internas, desde la AYTO se accede a INTERNET tal y como se muestra en la figura.

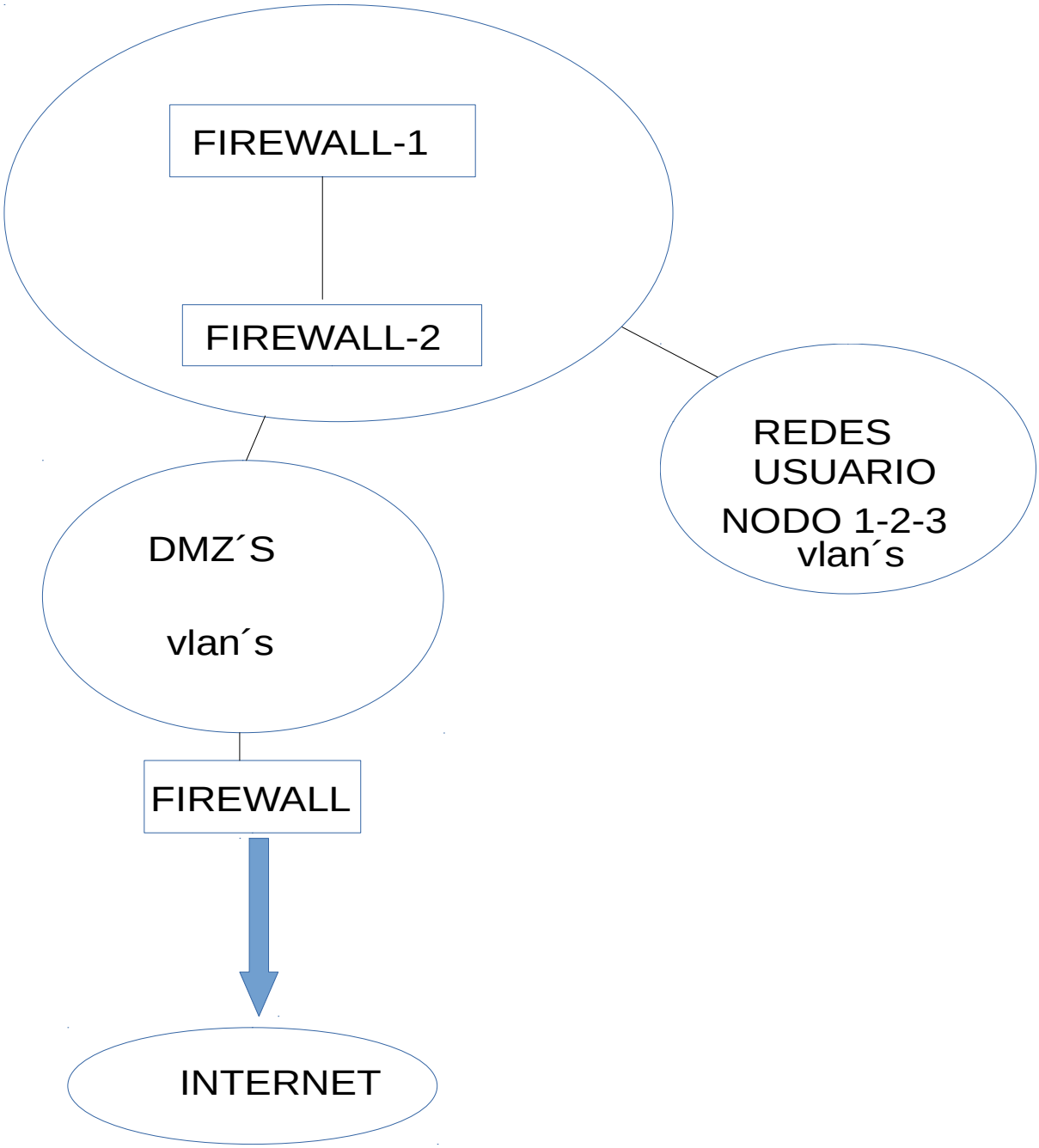


ARQUITECTURA FINAL

El nivel de routing permite la comunicación entre las distintas subredes que integran la arquitectura lógica de la la infraestructura de comunicación de datos.

La arquitectura futura se basa en la sustitución del modelo de conmutación, asociado con un cambio de los nodos de enrutamiento, pasando, de ser routers clásicos, a un cluster de Firewalls, consiguiendo , de este modo, una seguridad nativa.

Con ello se pretende que el cambio de conmutación de Nivel 3 a 2 vaya asociado, a un modelo de routing seguro. En este sentido, se deben tener en cuenta los accesos Inter.- VLAN´s.



- Los NODOS: 1, 2 y 3 basados en Switches Cisco ya no se comunicarán entre ellos a nivel 3. Lo harán a nivel 2 y a nivel de VLANs, que serán y estarán accesibles desde todos los nodos de la red troncal

- Se permitirá, si así se desea, que se puedan extender sin problemas las subredes del CPD de producción en el CPD de backup y viceversa.

- Las puertas de enlace de todas las subredes internas de la red AYTO serán la IP virtual de un cluster de FW´s (s firewalls)

- Desaparece el routing dinámico OSPF. La alta disponibilidad entre los enlaces que unen los distintos nodos de la red AYTO se hará mediante enlaces de fibra redundantes (recálculos de spanning tree).

Objeto del ejercicio

- Plantear un proyecto de migración por fases. Puntuación: 420 puntos
    - Planteamiento general de la Arquitectura. Futura: Gráfico de la arquitectura final
    - Proyecto de migración.
        - Reorganización y Definición de VLANS..
        - Elección de switches y otros elementos del universo Layer 2..
        - Configuración de las VLAN´s. Criterios a seguir.
        - Fases de configuración de las máquinas: paso a paso.
    - Migración de las redes: físicas a VLAN: paso a paso. Hacer referencia a los comandos más importantes para ello, (sin detalle).
    - Somero planteamiento del QoS: como y donde se implementaría
    - Arquitectura de routing;: donde y como se hace el routing interVLAN y hacia Internet, seguridad unificada, y las implantaciones necesarias para conseguirlo.

- Señalar que aporta esta arquitectura con respecto a la de Layer 3. Pros y contras. Motivarlo y poner ejemplos concretos. Puntuación: 90 puntos

- Señalar que problemas que pueden aflorar en una red multicamino (enlaces redundantes entres sedes) y las soluciones a implementar en cada caso. Puntuación: 90 puntos

SUPUESTO 2: DISEÑO DE UNA SOLUCIÓN DE COMUNICACIONES POR RADIO ENLACE. (200 puntos)

Situación de partida

La Depuradora de Araka, dependiente de AMVISA (Aguas Municipales de Vitoria), y sita en el "monte de Araka", no dispone de una conexión de datos de calidad a la red municipal . En la actualidad se "sale del paso" con conexiones 3G / 4G que resultan lentas y caras para los fines previstos. La Depuradora se halla ubicada en terreno militar y a un cota de 650 metros de altura.

Se plantea la necesidad de , al tratarse de una instalación estratégica, conectar dicha Depuradora a la red municipal de comunicaciones de datos en las condiciones que dicha catalogación exigen en cuestiones tales como integridad, disponibilidad..

Por su situación elevada y a 4 Kilómetros en línea recta del casco urbano, la posibilidad de echar fibra óptica hasta sus instalaciones es poco posible técnicamente y muy cara.

Por ello, se plantean alternativas de conectividad, que cumplan con una serie de requisitos técnicos, económicos y de calidad.

La Depuradora de Araka, alberga una serie de servicios que necesitan el uso de soluciones tecnológicas que, a su vez, necesitan comunicarse con la Red Corporativa Municipal , con la cual mantiene una serie de servicios activos:

- Telefonía Ip, servida por la centra de VoIp municipal sita en la Red Corporativa
- Aplicaciones municipales, que trabajan contra servidores centralizados en la Red Corporativa
- Conexión Centralizada a Internet para los usuarios corporativos.
- Conexión independiente a Internet del propio edificio de Depuradora para ciertos sensores que conectan con empresas y organismos externos de control.
- Transmisión desde diversos sensores a un SCADA sito en las oficinas centrales de AMVISA, en la calle Puerto Rico, conectadas a red municipal).

PLANO GENERAL – ARAKA – CASCO URBANO DE VITORIA-GASTEIZ. En el Plano de Vitoria con Araka a la vista se aprecia la distancia de la Depuradora al Casco Urbano de Gasteiz y, por lo tanto, al entramado de fibra óptica que conforma la Red Corporativa uniendo edificios de servicios municipales. **(anexo I)**

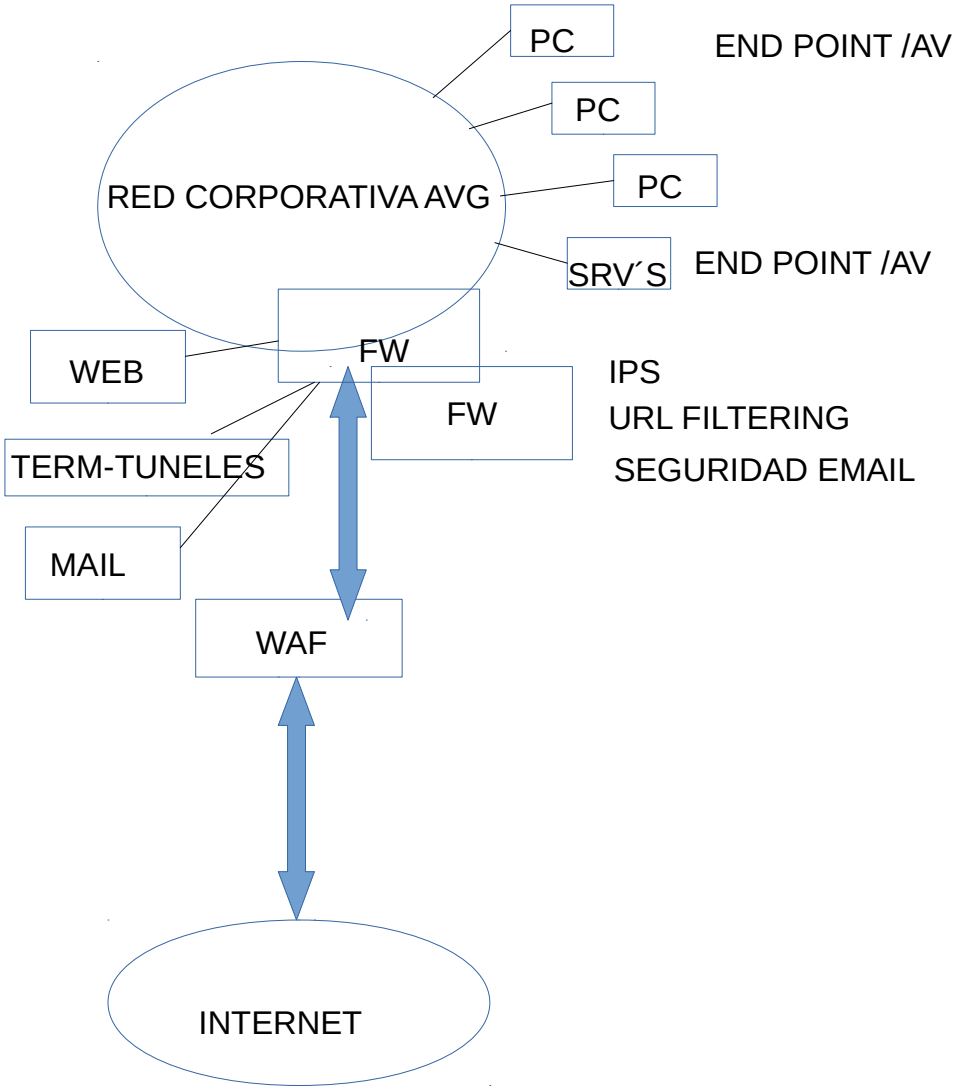
PLANO ESPECIFICO- GASTEIZ – EDIFICIOS – FIBRA. En este Plano de Vitoria se aprecian diferentes edificios municipales (propiedad municipal y susceptibles de ser usados para montar infraestructuras). Las líneas amarillas marcan los ramales de fibra óptica que unen dichos edificios y conforman la red de datos municipal. **(anexo II)**

Objeto del ejercicio

- Motivación de uso de la tecnología de radio enlace sobre otras tecnologías (20 puntos)
- Uso de banda licenciada o libre: motivación. Cuidados especiales a tener en cuenta en este apartado. (14 puntos)
- Seguridad aplicable en la transmisión de los datos (si procede). (20 puntos)
- Diseño físico de la solución. Montaje, antenas, alimentación, transceivers, conmutación. (50 puntos)
- Diseño lógico: teniendo en cuenta que TODOS los servicios de datos son servidos desde la Red de Comunicaciones Corporativa del Ayuntamiento de Vitoria-Gasteiz, en la cual se hallan las salidas a Internet Corporativo, los servidores de Aplicaciones municipales y el SCADA. En el diseño lógico se incluirá QoS si se considera necesario (52 puntos)
- Integración en la red municipal. Como se llevaría a cabo? Pasos, aspectos a tener en cuenta, problemática, soluciones (30 puntos)
- Pruebas a realizar. Relación sin entrar en detalle. (8 puntos)
- Documentación a elaborar. Relación sin entrar en detalle. (6 puntos)

SUPUESTO 3: ARQUITECTURA DE UNA VERTICAL DE SEGURIDAD HOMOGENEA. (200 puntos)

En el marco de una organización compleja , como el Ayuntamiento de Vitoria-Gasteiz (en adelante AVG), se han detectado, tras una auditoría de seguridad, diversos posibles vectores de ciber ataque: correo electrónico, dispositivos de almacenamiento externo,, Web, los puestos de trabajo (usuario final o estaciones de trabajo-servidores) y un terminador de túneles IPSEC, que pueden poner en peligro la integridad de la organización



.

Esta organización dispone de diversos elementos de protección: firewalls, anti virus, sondas, IPS… que se han ido integrando en la estructura de seguridad a lo largo del tiempo.

La información que obtenemos de todos estos elementos es grande y variada, aportando los datos necesarios para llevar a cabo las modificaciones necesarias para cubrir las necesidades, en lo que a seguridad se refiere, del AVG:

En este marco, la necesidad de tener una gestión integrada homogénea de todos los dispositivos, herramientas o sistemas de seguridad se hace imprescindible para una adecuada resolución de problemas y una prevención proactiva adecuada.

La diversidad de productos de seguridad, formatos de datos, protocolos , así como el hecho de que dichos datos sean , en ocasiones, referentes a productos concretos con fabricantes distintos, hace que la disparidad de dichos datos haga difícil un tratamiento homogéneo, y, por lo tanto, la obtención de conclusiones del cruce de dichos datos para la toma de decisiones que nos permitan un rendimiento óptimo (proactivo incluso).

Con la falta de coherencia y de homogeneidad en los productos, la arquitectura, los datos, y por lo tanto de los resultados de la conjunción de todos los datos extraíbles de estos dispositivos (hard y soft) no son comparables o inteligibles entre ellos.

En aras de una mayor efectividad y simplificación de los procesos de seguridad interna y periférica se pretende construir una arquitectura de seguridad sólida y homogénea que nos permita tener un punto central de control de la seguridad de la organización (tipo SIEM).

Para ello, se pretende unificar en criterios, productos y formatos de datos todas las protecciones de la Organización para todos y cada uno de los vectores posibles de ataque y en toda la vertical:

- La protección del puesto de trabajo: sea con una herramienta de end point, anti virus, ambas combinadas etc… Seguridad física – USB´s..
- Seguridad perimetral: con todo lo que puede conllevar: Sand Box, IPS, IDS…
- WAF (si se estima necesario).
- Seguridad Correo Electrónico: Alternativas?
- …

Objeto del ejercicio

- Plantear una arquitectura de seguridad unificada y homogénea teniendo en cuenta, como mínimo, los vectores indicados. Puntuación: 100 puntos,
- Definir las interrelaciones de datos entre cada elemento de la arquitectura. Puntuación: 30 puntos
- Plantear las herramientas de gestión, control, logging y monitorización. Poner ejemplo concreto de herramienta/s. Puntuación: 20 puntos,
- ¿Como la homogeneidad de tecnologías/productos ayudaría a la proactividad? Poner un ejemplo concreto. Puntuación: 20 puntos,
- En cada elemento, explicar muy someramente las amenazas (sin llegar a un nivel técnico profundo del tipo de amenaza) de las que protegería. Puntuación: 20 puntos,
- Herramientas o tecnologías que aporten un valor añadido: uso de tokens, doble factor de autenticación u otros. En que punto y para qué? Puntuación: 10 puntos.