www.DarFe.es

"Charlas sobre Ciberseguridad"

(módulo: cursos On-Line Ciberseguridad ***moodle.darFe.es****)*

TEMA 8

Ciberdefensa: nuevos conceptos, nuevas metodologías, nuevos desafíos.

(martes 31 de octubre de 2017)

Índice

1. INTRODUCCIÓN

Esta es la última de nuestras charlas. En la misma, como cierre, iremos realizando la consolidación de varios conceptos ya tratados y a su vez los integraremos con nuevas tecnologías e ideas que están apareciendo y merecen la pena tener en cuenta.

2. OBJETIVO

Cerrar este ciclo con una serie de reflexiones e integrando gran parte de lo visto a través de un conjunto de imágenes.

3. TEMARIO Y FECHAS DE TODO EL CICLO 2017

A continuación se presentan la totalidad de las charlas que conforman este ciclo durante el año 2017.

Temario y fechas

Nº	Tema de la charla	Fecha
1	**Presentación, conceptos y situación de Ciberseguridad. *¿De quién nos defendemos?***	**Jueves 30 de marzo**
2	**Estrategias de Ciberseguridad en grandes redes (*Seguir y perseguir - proteger y proceder*)**	**Jueves 27 de abril**
3	**Ciberdefensa en profundidad y en altura (*la conquista de las cumbres*)**	**Jueves 25 de mayo**
4	**Ciberseguridad: La importancia de los procesos.**	**Jueves 29 de junio**
5	**Ciberseguridad: Plataformas / infraestructuras de Seguridad en Red**	**Jueves 27 de Julio**
6	**Ciberseguridad: Cómo son las entrañas de esta gran red mundial**	**Jueves 31 de agosto**
7	**Ciberseguridad: empleo de SOC y NOC**	**Jueves 28 de setiembre**
8	**Ciberseguridad: la importancia de saber gestionar "Logs"**	**Martes 31 de octubre**

4. PRESENTACIÓN DEL TEMA DE HOY

Resumen del tema

El objetivo de este último tema es consolidar la mayoría de los conceptos ya tratados anteriormente y reforzarlos con nuevas ideas.

Como se verá, en esta parte el desarrollo será eminentemente gráfico, para reforzar y cerrar conceptos de la forma más clara posible.

Por esta razón, la estructura de este final, es diferente al resto del libro, presentándolo de la siguiente forma.

- Conceptos ya difundidos:
  - Defensa en profundidad y en altura.
  - Dinámica de la defensa.
  - De "Proteger y proceder" a "Seguir y Perseguir" (**RFC-1244**).
  - Ciber operación de Acción retardante.

- Nuevos conceptos y desafíos:
  - Compartimentación de redes (la familia IEEE-802.x).
    - *Reducir superficie de ataque.*
    - *Arquitectura de red de confianza cero.*
    - *Organización por tecnologías.*
    - *Granularidad.*
    - *Exfiltración de datos.*
    - *Gestión de actualizaciones.*

- *Capacidad de reacción.*

- Ruido en la red.
- Resiliencia.
- Virtualización (de host y de redes).
- Delegación y segregación de responsabilidades y funciones.
- Contra inteligencia.
- Juegos de ciberguerra.

7.1. Presentación.

Nuestras infraestructuras de red y TI se nos están haciendo cada vez más "pesadas".

En los últimos años, día a día se van incrementando el nivel de actualizaciones, parches, dispositivos de seguridad, de detección, de monitorización, de prevención y detección de ataques, de antivirus, antiDDoS, antispam, antiphishing, anti…..

Llevando una vez más la seguridad informática al terreno militar, esto me hace acordar a las campañas de los grandes ejércitos de la historia, donde en virtud de los miles de combatientes, necesitaban una cantidad generalmente superior de infraestructura logística, de apoyo, de seguridad en sus puntos de conquista, de salvaguarda de sus fronteras y flancos, de fábricas y almacenes de material, de medios de transporte, etc. Me atrevería a afirmar que la totalidad de estos casos sucumbieron pues no podían soportar esta carga colateral a la acción de guerra en sí. Si se analiza la historia militar, detrás de todos ellos hubo verdaderos estrategas militares pero su ambición los llevó a los límites del concepto de "seguridad" y fueron siendo derrotados por no ser capaces de mantener estas enormes infraestructuras de guerra.

Hoy nuestras infraestructuras de red y TI se nos presentan como algo similar. Nos encontramos batallando en esta Ciberguerra sobre un escenario sin fronteras, obligados a exponer cada vez más nuestros

recursos, incorporando nuevos elementos, aplicaciones, protocolos de comunicaciones, información que en muchos casos no llegamos a conocer a fondo pues no damos abasto, dejando con ello cada vez más potenciales amenazas.

El Ciber enemigo opera como si fuera "guerrilla". No es un enemigo convencional, no le aplica ninguna de las leyes de esta guerra (leyes y regulaciones nacionales y/o internacionales). Nos ataca con "golpes de mano" precisos, no da la cara, tiene organización celular, está al margen de la ley, tiene muy fácil las medidas de velo y engaño, de enmascaramiento, de evasión y escape.

Nuestra estrategia de "Ciberdefensa" no puede seguir siendo la convencional o clásica, debemos operar dentro de la ley con: nuevos conceptos, nuevas metodologías, nuevos desafíos.

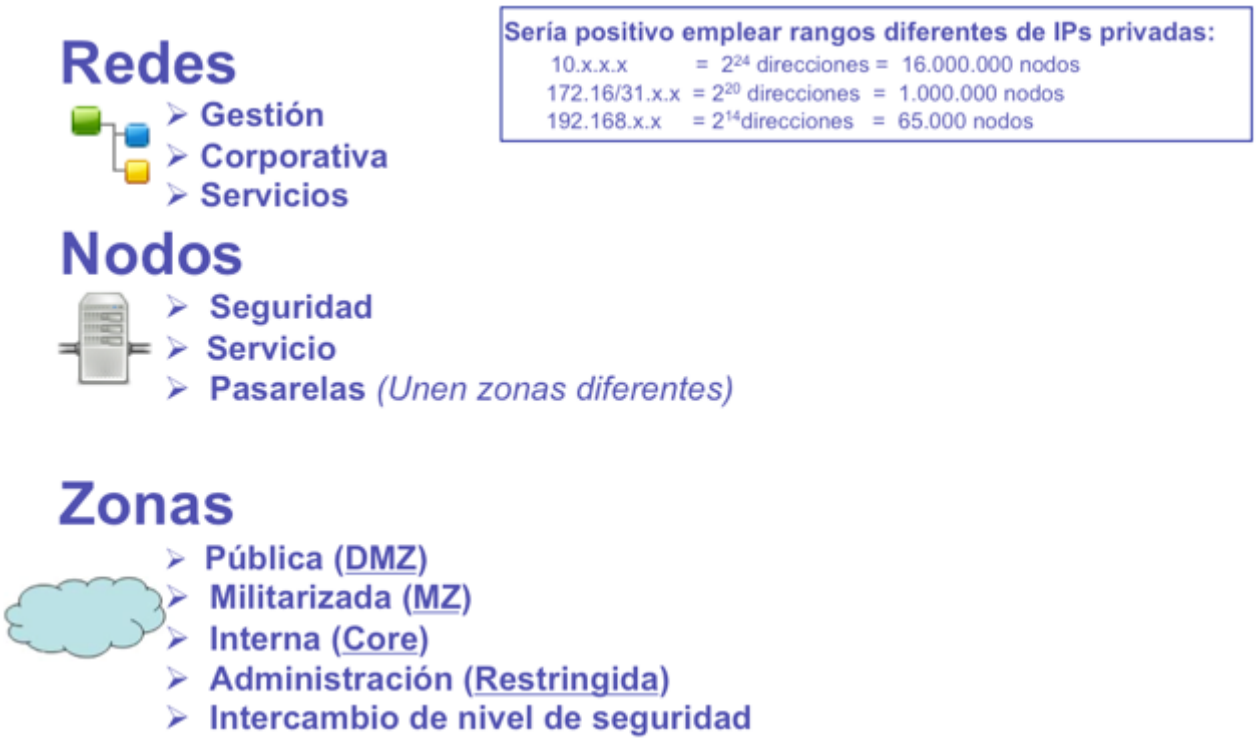
No profundizaremos más sobre conceptos que ya han sido presentados desde hace años, sólo los mencionaremos brevemente.

7.2. Nuestra visión del problema.

Vamos a comenzar el tema, definiendo la idea de "Redes, Nodos y Zonas".

- **Red**: medio físico que una 2 o más nodos (*cero saltos IP*).
- **Nodo**: Elemento direccionable por direccionamiento IP (*Posee 1 o más direcciones de igual o diferente tipo*).

  Zona: Área que mantiene el mismo nivel de seguridad.



Como detalle de la experiencia, es una muy buena práctica a la hora de diseñar redes, hacer uso de lo que nos establece la **RFC 1918** en cuanto a las direcciones IP privadas.

Si es posible, se pueden asignar diferentes rangos basados en alguna cierta lógica como puede ser a título de ejemplo:

10.0-7.x.x/11 zona central,

10.8-15.x.x/11 zona A,

10.16-23.x.x/11 zona B,

10.24-31.x.x/11 zona C

……..

10.128-135.x.x/11 zona N,

etc…

Para los enlaces punto a punto, o punto multipunto, entre estas zonas hacer uso de otro rango, por ejemplo:

192.168.0-7.x/19 para enlaces de la zona central,

192.168.8-15.x/19 para enlaces de la zona A,

192.168.16-23.x/19 para enlaces de la zona B,

192.168.24-31.x/19 para enlaces de la zona C,

……

192.168.128-135.x/19 para enlaces de la zona N,

etc…

Se puede dejar el rango 172.16-31.x.x para cualquier otra red "especial" que deseemos.

Esta asignación de direccionamiento IP, desde el punto de vista de seguridad es muy importante, pues a medida que el trabajo en la red se va haciendo cotidiano, es muy fácil identificar cualquier dirección IP, con una región geográfica, un edificio, una planta del mismo, un área de trabajo, etc. Si consideramos este detalle, cuando se deba analizar tráfico, reglas de un FW, configuración de rutas, listas de control de acceso, etc. Cualquier decisión que se tome al respecto será mucho más sencilla, clara y finalmente segura.

Volviendo a nuestros conceptos de "defensa en profundidad" presentados en el capítulo 4, retomamos a continuación la imagen de zonas de red, en la cual representamos, las diferentes "líneas defensivas" y genéricamente los dispositivos que nos proporcionan la información y las comunicaciones necesarias para el funcionamiento de las infraestructuras.

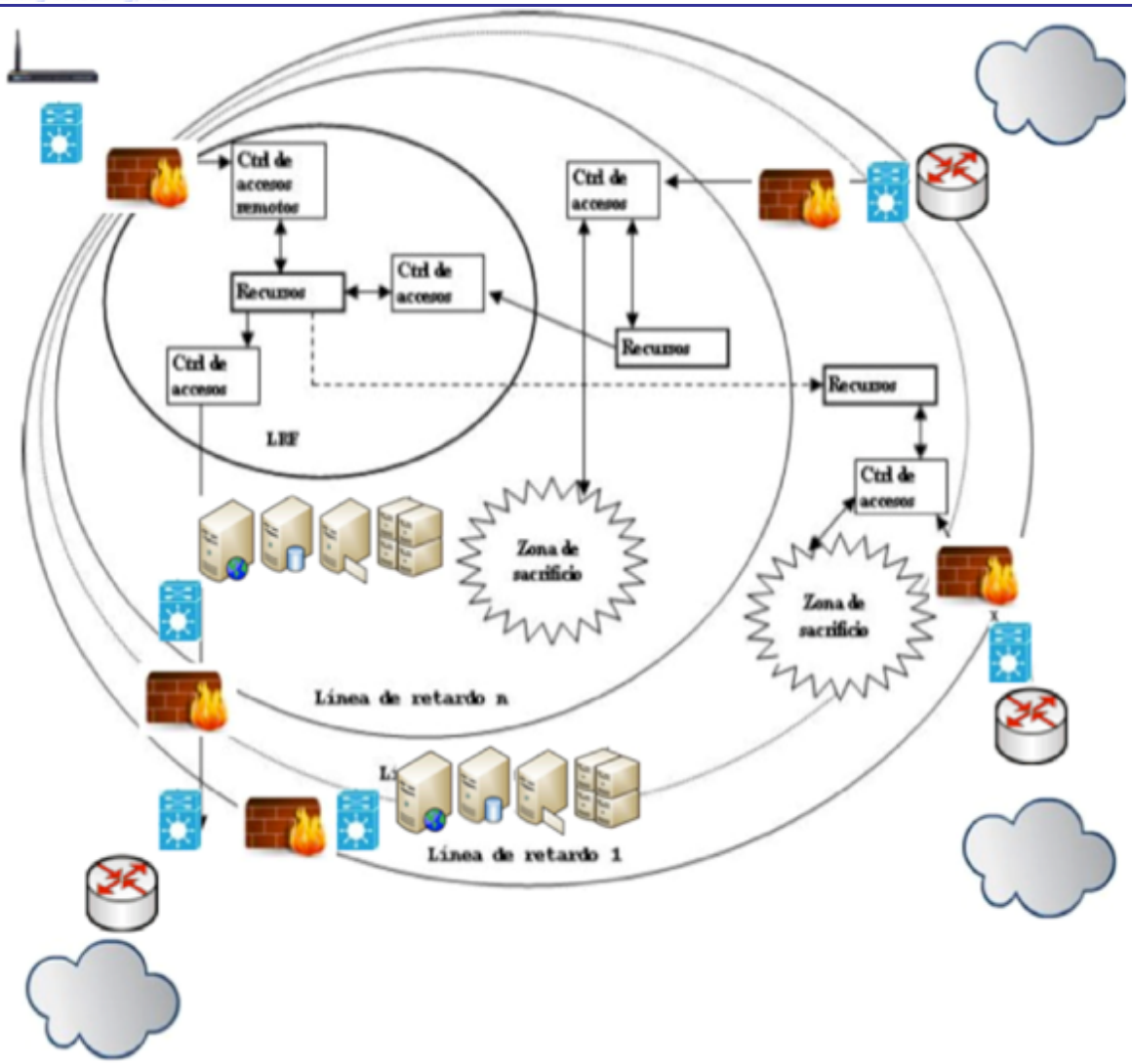


Imagen de zonas de red

Si sobre la imagen anterior, deseamos continuar el nivel de detalle, la realidad es que cada uno de estos dispositivos y/o zonas de red, se comunican a través de "**medios físicos**". Un medio físico, como su palabra lo indica es algo "tangible" que permite el tránsito de la información, dependiendo de las características físicas de este medio, la información viajará por medio de una señal óptica o electromagnética. En la actualidad sólo existen los siguientes medios físicos:

- Cable (*UTP, STP, Coaxial, etc.).*
- Fibra óptica (*monomodo y multimodo*).

- Radio (Microondas, satélite, radioenlaces, LF, HF, VHF, etc.)
- Guías de onda (*en general sólo empleadas en laboratorio o dentro de los sistemas de antena*).

Para profundizar sobre cualquiera de ellas, aconsejamos la lectura del capítulo 3 del libro "**Seguridad por Niveles**".

En definitiva, estos medios físicos, interconectarán los dispositivos, bajo tres tipos posibles:

- Punto a punto.
- Punto a multipunto.
- Multipunto a multipunto.

Estas conexiones llevadas al plano real, las veríamos tal cual se presentan en la imagen siguiente.

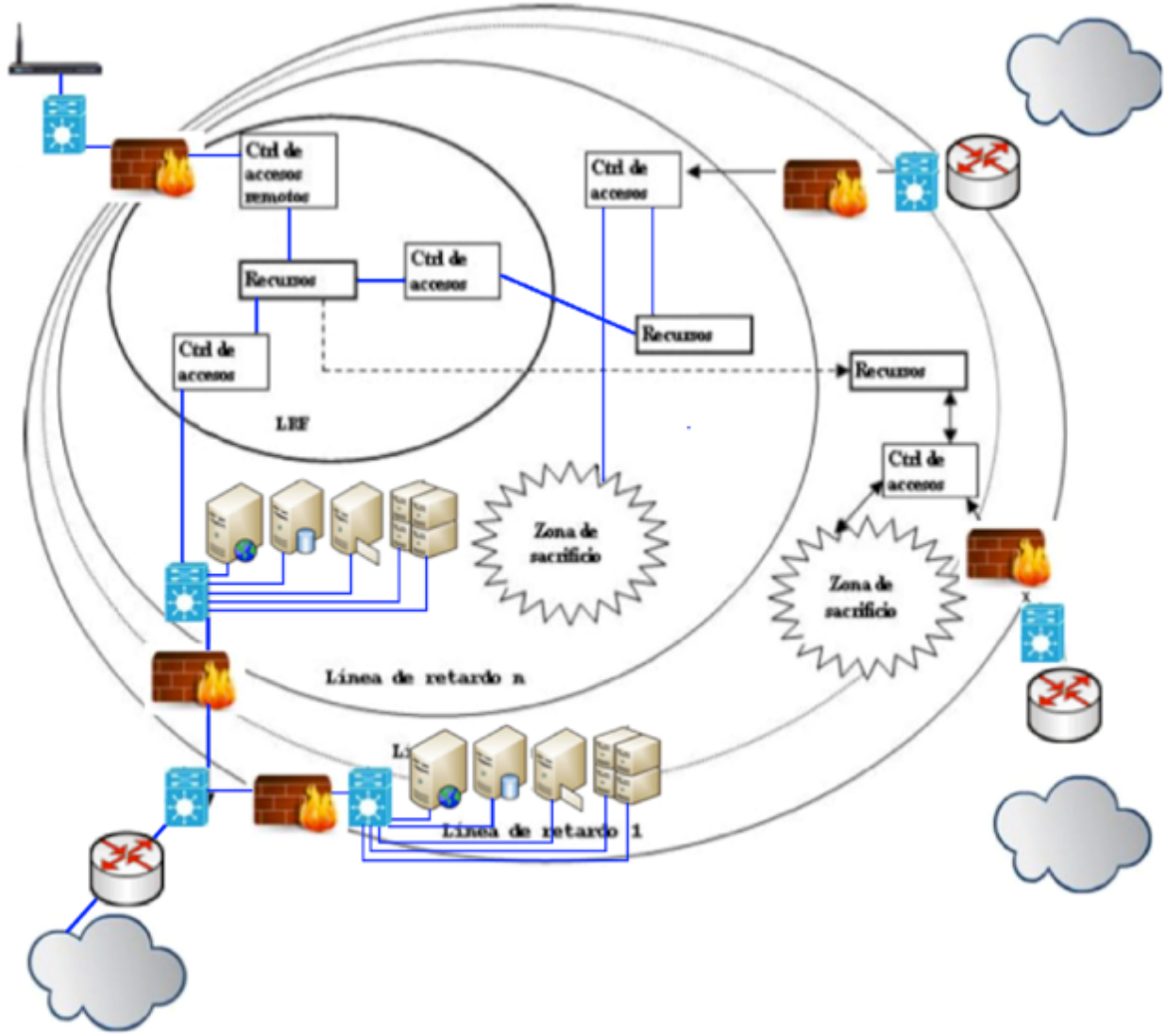


Imagen de conectividad a nivel físico

Siguiendo con nuestra "consolidación" de conceptos, si recordamos lo tratado en el capítulo **5. Ciberdefensa en profundidad y en altura** (la conquista de las cumbres) de este libro, el tema se encontraba dividido en dos líneas de avance:

1) Planos de altura (niveles TCP/IP)

2) Planos de Segmentación en redes de: Gestión y Servicio.

Los niveles del modelo TCP/IP, una vez más, si los graficamos desde la realidad de nuestras redes, en definitiva, van asociados directamente con los dispositivos que empleamos en ellas. Como siempre hacemos mención, en virtud de la potencia de la electrónica actual los diferentes

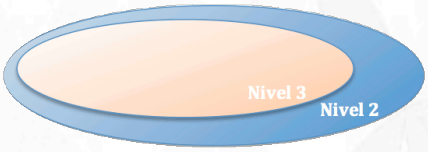
dispositivos, van asumiendo cada vez más funcionalidades, ocupando "capas" que no fueron su función original, por lo tano podemos discutir si hoy en día es taxativamente así, pero si somos rigurosos conceptualmente, en concreto la relación nivel/dispositivo es:

- **Nivel 2**: Switchs.

  Podemos  representarlos también como si fuera una "carta topográfica", en la cual por medio de "curvas de nivel, se representan las diferentes cotas de altura, por ejemplo, de la siguiente forma:

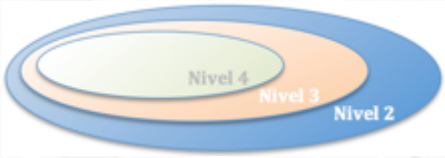
- **Nivel 3**: Routers.

  Idem anterior:



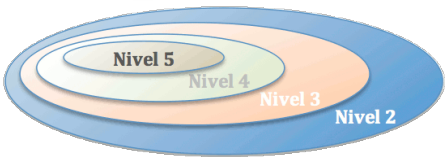
- **Nivel 4**: Firewalls.

  Idem anterior:



- **Nivel 5**: Servidores.

  Idem anterior:



Ahora, si queremos reflejar este tipo de representación, podemos hacerlo de acuerdo a la imagen que sigue.

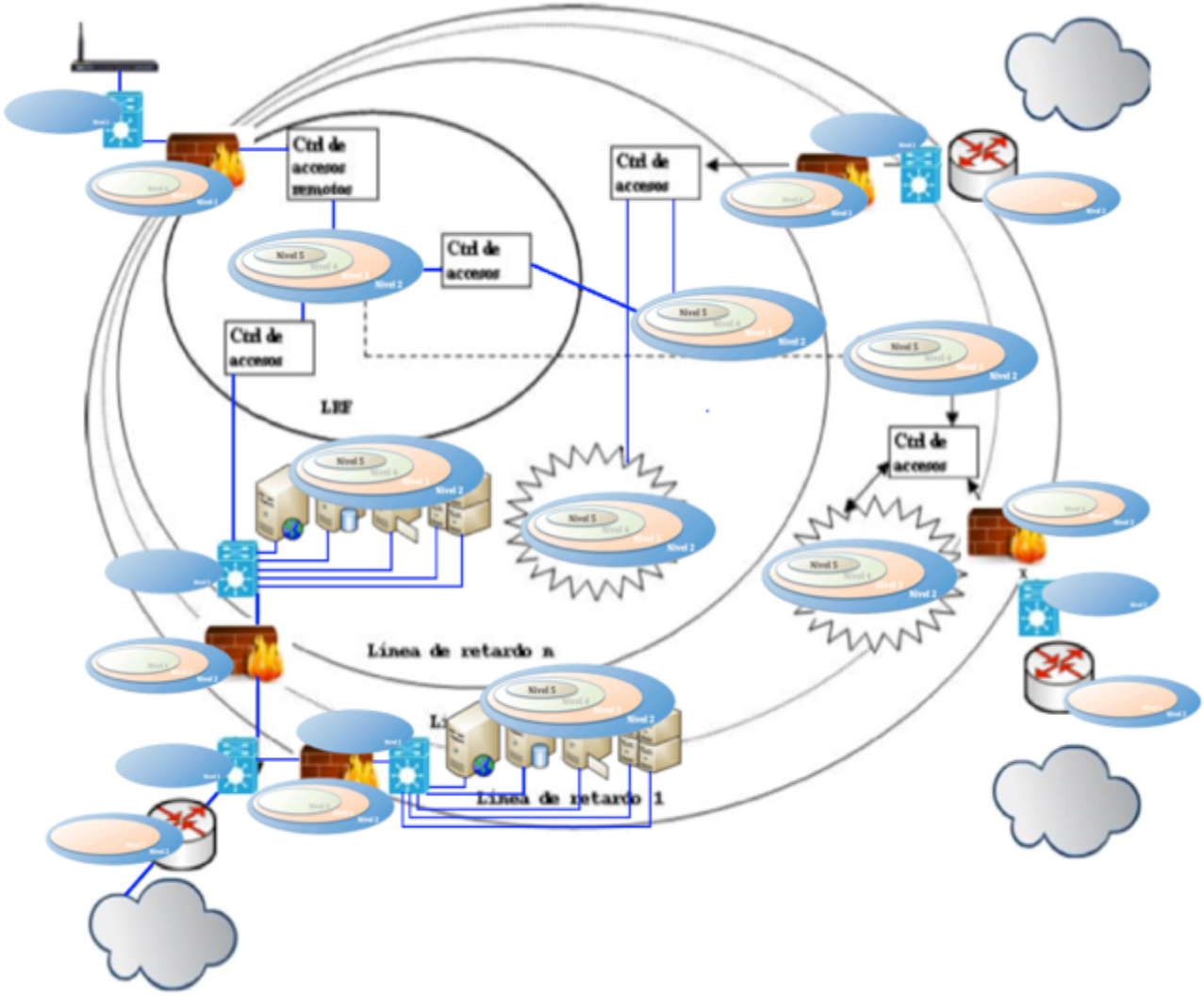


Imagen de planos de altura según niveles TCP/IP

Si avanzamos sobre esta misma imagen, pero sumándole ahora los "Planos de Segmentación en redes de Gestión y Servicio", tal cual acabamos de recordar de este capítulo 5, podríamos presentarlo de acuerdo a la imagen que se ve a continuación.

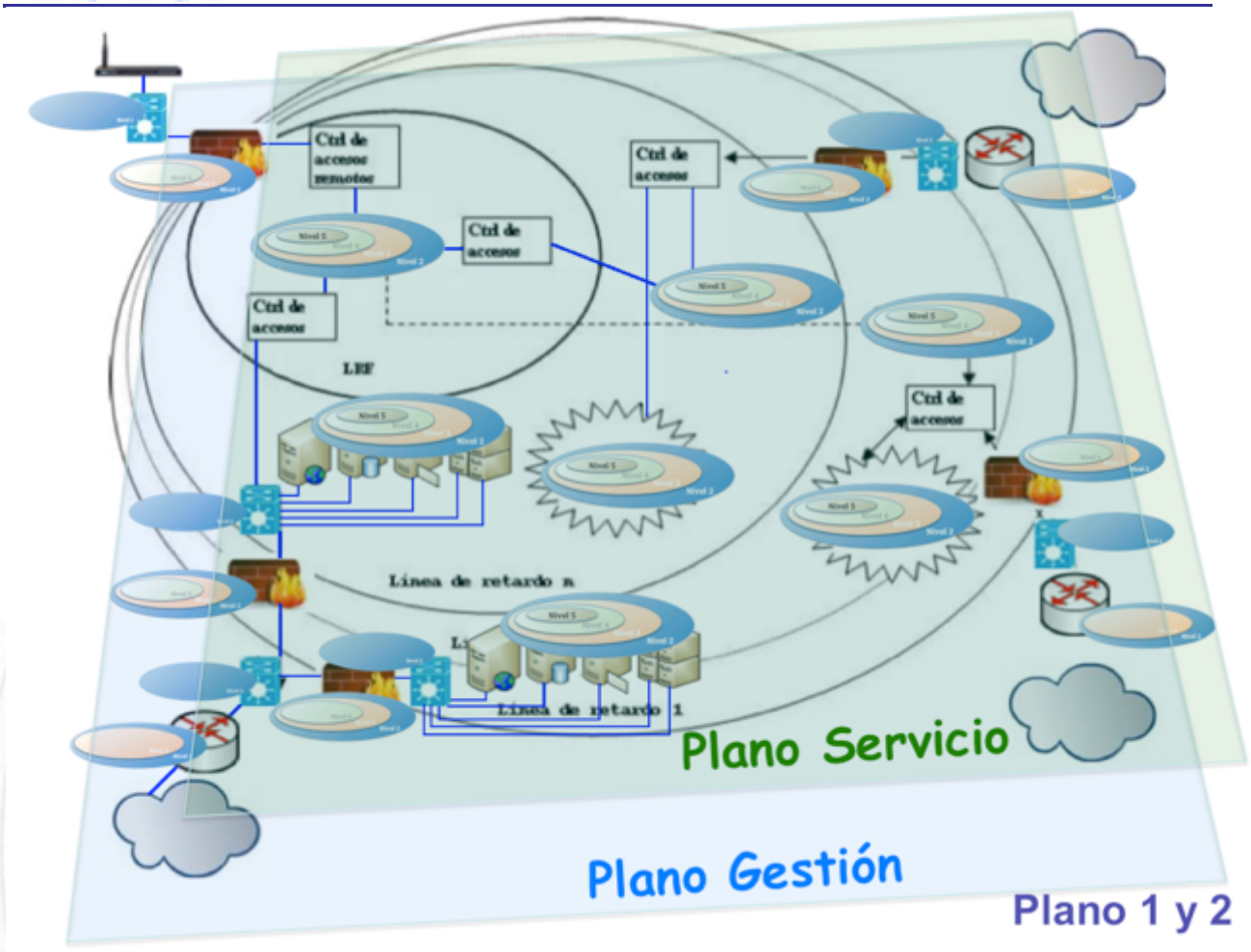


Imagen de planos de altura según redes de "Gestión" y "Servicio"

Con las dos imágenes anteriores tenemos una visión clara y representativa de cómo podemos tratar y definir las diferentes "alturas" desde el punto de vista de la seguridad de nuestras infraestructuras.

Si seguimos desarrollando gráficamente los conceptos de los capítulos anteriores, podemos presentar lo tratado en el capítulo **4. Estrategias de Ciberseguridad en grandes redes** (Seguir y perseguir - proteger y proceder).

Supongamos inicialmente un "vector de ataque" (*que en la gráfica que sigue, lo podemos ver en el extremo inferior izquierdo*). Cuando nuestra infraestructura y recursos humanos no están lo suficientemente preparados, debemos plantearnos la estrategia de

"Proteger y proceder", tal cual se representa en la imagen, lo único que podríamos hacer es ir desconectando enlaces (en color rojo) y apagando dispositivos (también en rojo). Recordemos (o repasemos) lo presentado en el punto **4.1. Planteo inicial** de este libro.

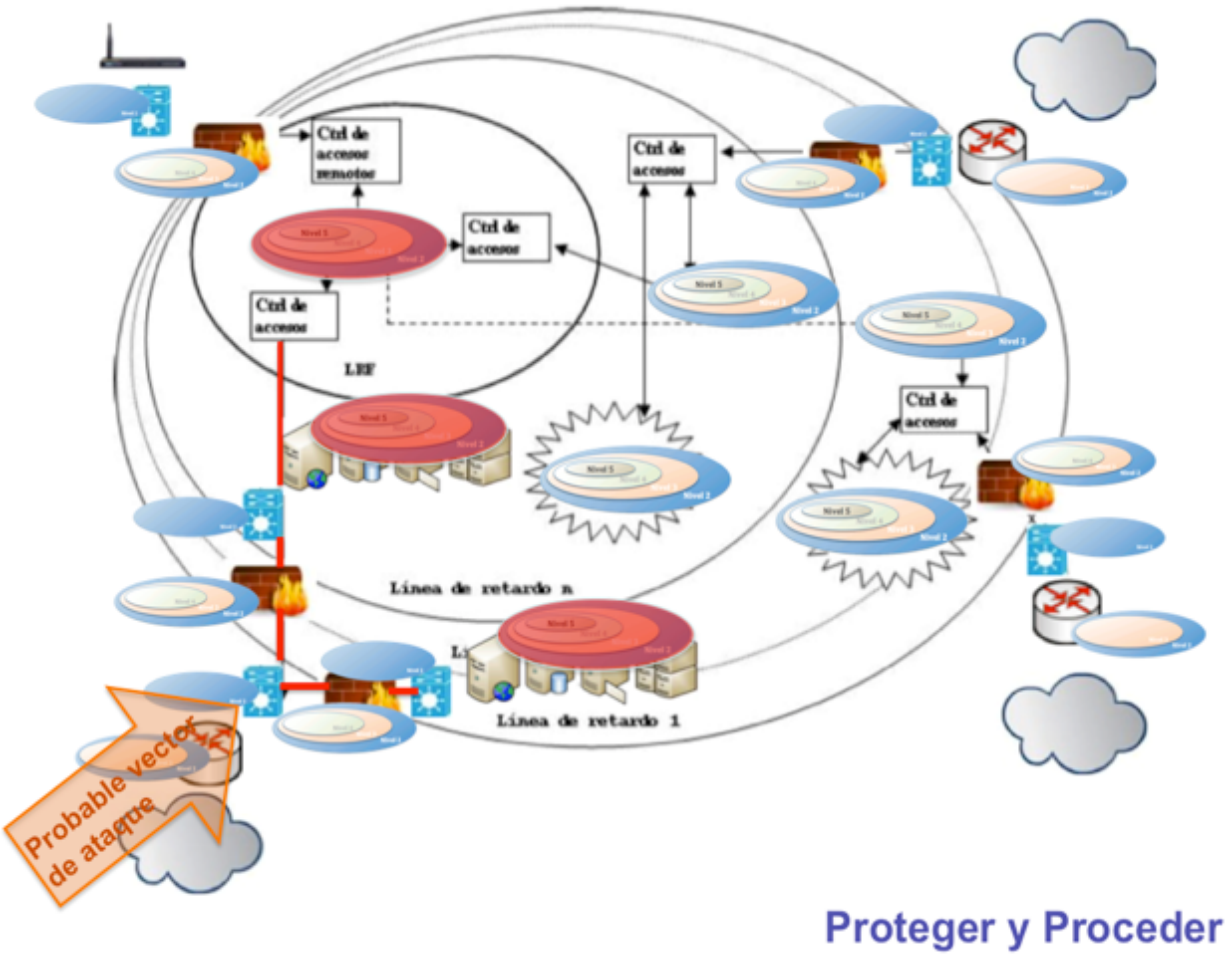


Imagen vector de ataque 1, Proteger y Proceder

Manteniendo los conceptos del capítulo 4, supongamos ahora otro vector de ataque (*que en la gráfica que sigue, lo podemos ver en el extremo inferior derecho*). Cuando nuestra infraestructura y recursos humanos ***sí*** están lo suficientemente preparados, podemos entonces plantearnos la estrategia de "Seguir y perseguir". A través de esta postura, como ya mencionamos, podremos **llegar a la raíz del problema** y operando adecuadamente erradicarlo definitivamente.

Si hemos trabajado en cada uno de los niveles, nuestra respuesta podrá ser también en cada uno de ellos y estaremos en capacidad de "Monitorizar", "Mantener", "Almacenar datos", "Prevenir", "Evaluar", "Decidir" y hasta adoptar "Contramedidas" generando nuevas reglas en los FWs, Routers, y sistemas AntiDDoS, instalando nuevos parches y actualizaciones de seguridad, y finamente adoptando todo el conjunto de medidas que haga falta.

Esta metodología de gestión de incidentes es la que se representa en la imagen que sigue.

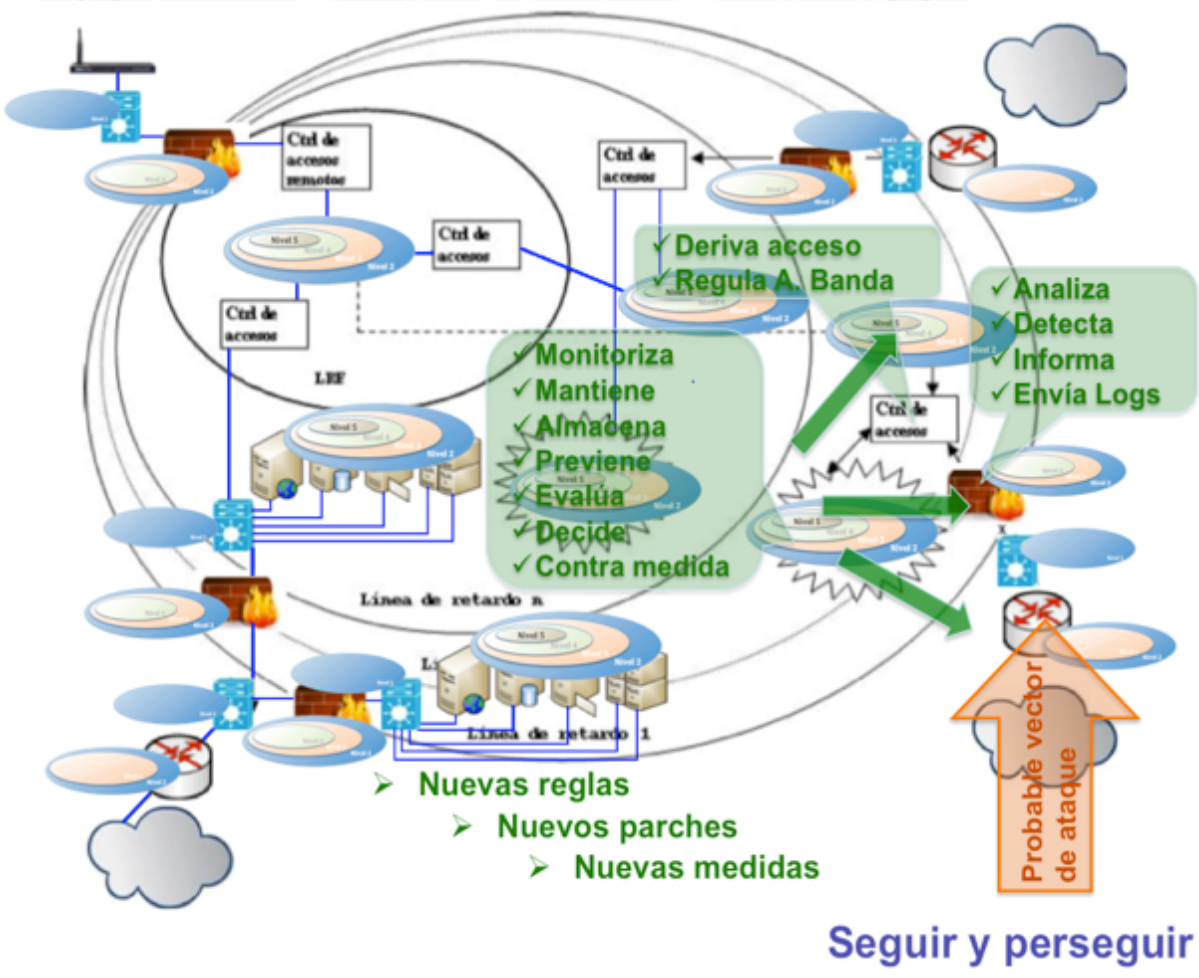


Imagen vector de ataque 2, Seguir y perseguir

En las dos imágenes que siguen, solamente se representan ambos escenarios y, con la intención de hacer repaso de conceptos, se hace hincapié en los conceptos fundamentales que nos pueden llevar a adoptar una u otra estrategia.

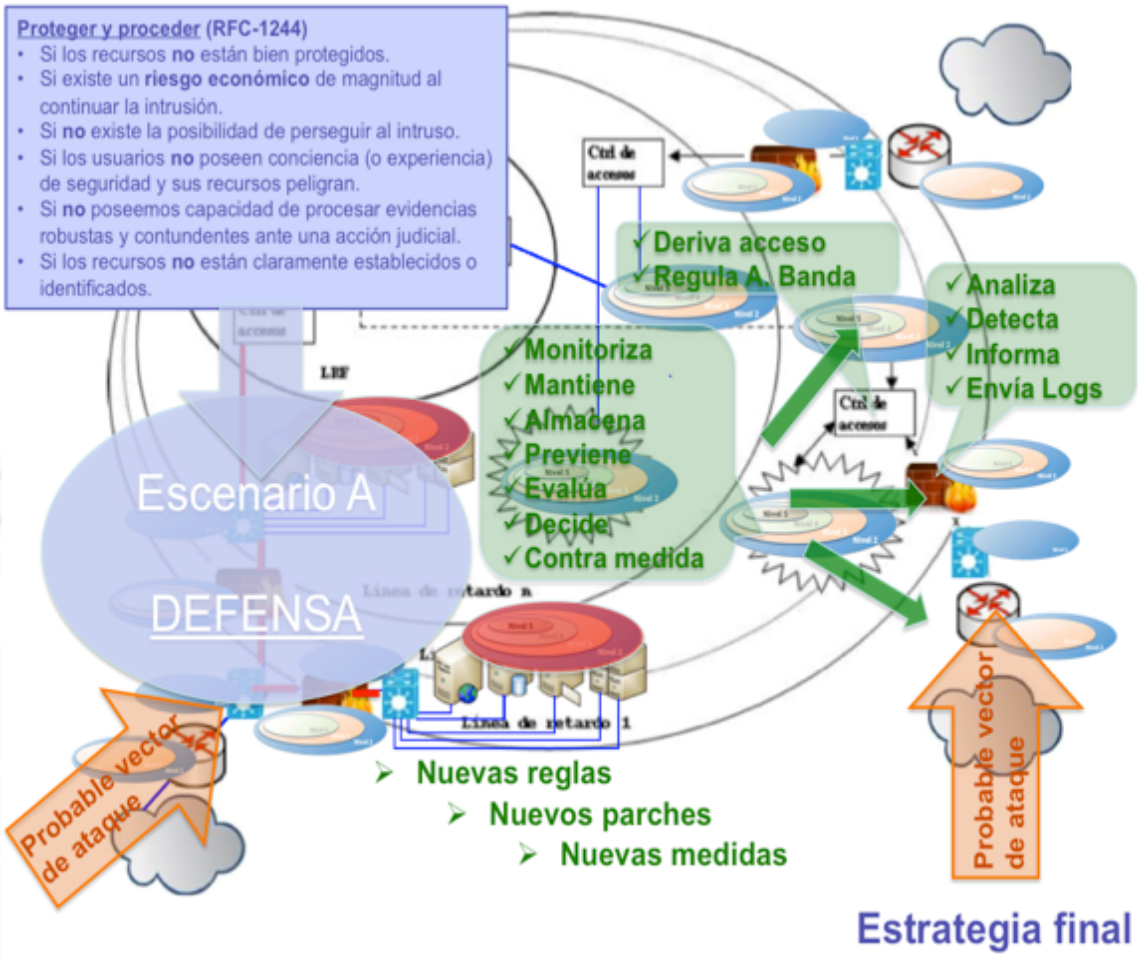


Imagen vector de ataque 1, conceptos de Proteger y Proceder

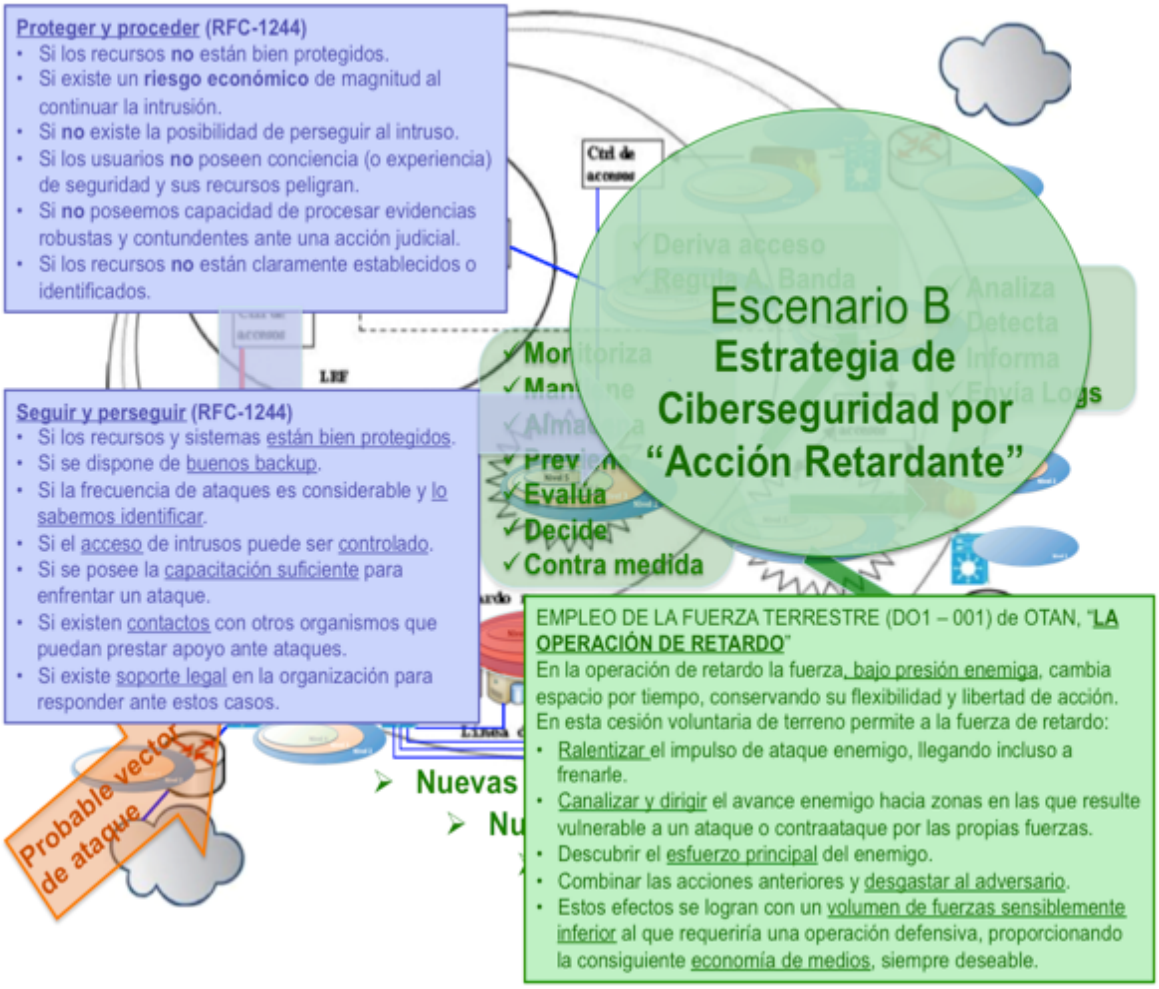


Imagen vector de ataque 2, conceptos de Seguir y perseguir

7.3. *Análisis por zonas.*

Considerando los conceptos del inicio de este capítulo "Redes, Nodos y Zonas", vamos a avanzar con más detalle sobre las diferentes "Zonas" que podemos considerar en nuestras redes.

Hasta ahora siempre nos hemos basado en nuestro modelo de "defensa en profundidad" sobre una arquitectura de rede tipo "capas de cebolla", en la cual a medida que profundizamos hacia el corazón de nuestra arquitectura vamos incorporando mayores exigencias de seguridad. Esta postura implica que SIEMPRE que deba decidir sobre la ubicación de cualquier tipo de dispositivos, deba evaluar su función y los servicios que vaya a prestar, sobre esta base, definir las exigencias

a las que se le someterá desde el punto de vista de la seguridad, y finalmente, en la medida que cumpla o no cada una de ellas, se le deberá asignar un "rating" o un valor que le permitirá o no estar conectado (o ser visible o alcanzable) desde una zona un otra.

Este conjunto de medidas y acciones es lo que dará origen a un verdadero plan de "Segmentación de redes". Si se desea profundizar en este tema, aconsejamos deis una mirada a un artículo que está publicado en Internet desde hace varios años "**Matriz de Estado de Seguridad**" (http://darfe.es/joomla/index.php/descargas/summary/5-seguridad/43-matriz-de-estado-de-seguridad).

Si hemos logrado valorar el nivel de seguridad de nuestros dispositivos y podemos identificar claramente en cuál de las zonas de nuestra red puede o no puede ser conectado, evidentemente nos surgirá necesidad de implementar medidas, interfaces o dispositivos que "permitan" o "nieguen" la visibilidad para cada IP/puerto de cada uno de los elementos de todas las zonas.

Estas interfaces o puntos de comunicación entre zonas de diferentes niveles de seguridad, en definitiva, terminarán siendo "interfaces" que se encuentran física o virtualmente uniendo zonas. Esto es lo que denominaremos "**Zonas de intercambio de Niveles de Seguridad**", y es importante que las visualicemos como "Zonas". En la realidad serán routers, firewalls, VPNs, host con más de una interfaz de red, conexiones dentro de un VMCenter, etc. Pero insistimos, veámosla SIEMPRE como "**Zonas**" para que quede claro que, en ese tramo de cable, en las bocas de ese switch, entre las interfaces de ese router, o dentro de ese "rack" de comunicaciones existe una "Zona" en la cual podemos "regular" el paso entre dos niveles de seguridad diferentes.

De forma gráfica, podemos representarla, por ejemplo, como la imagen que sigue.

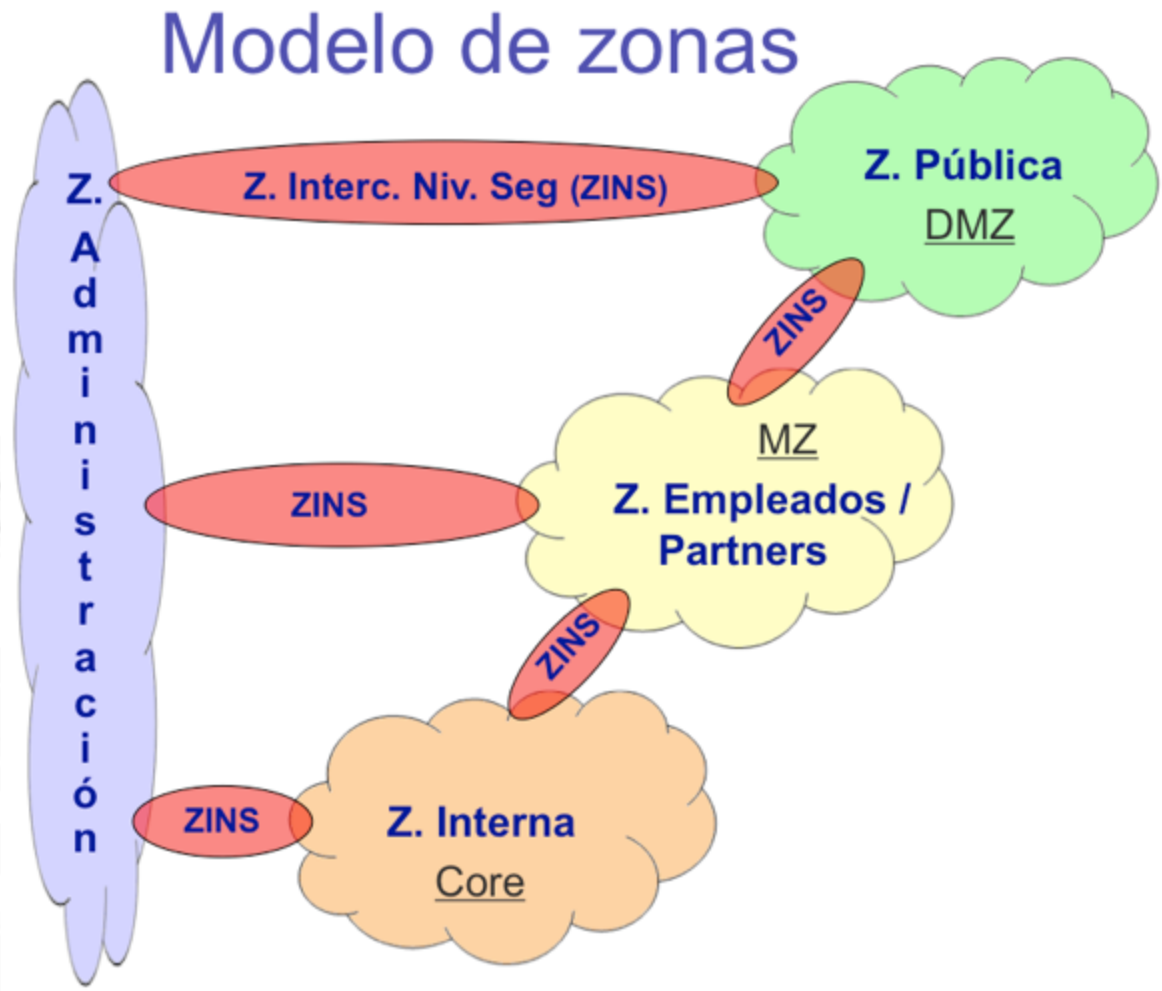


Imagen modelo de zonas

Si tenemos claro la función y los servicios que ofrecen los dispositivos y plataformas de cada una de esas zonas, entonces podemos aplicar una buena política de "Autenticación" y "Gestión de Accesos", para definir con total claridad los usuarios, roles y grupos que podrán o no acceder a cada una de ellas.

La imagen que sigue, es un ejemplo de cómo podríamos representar este control de accesos.

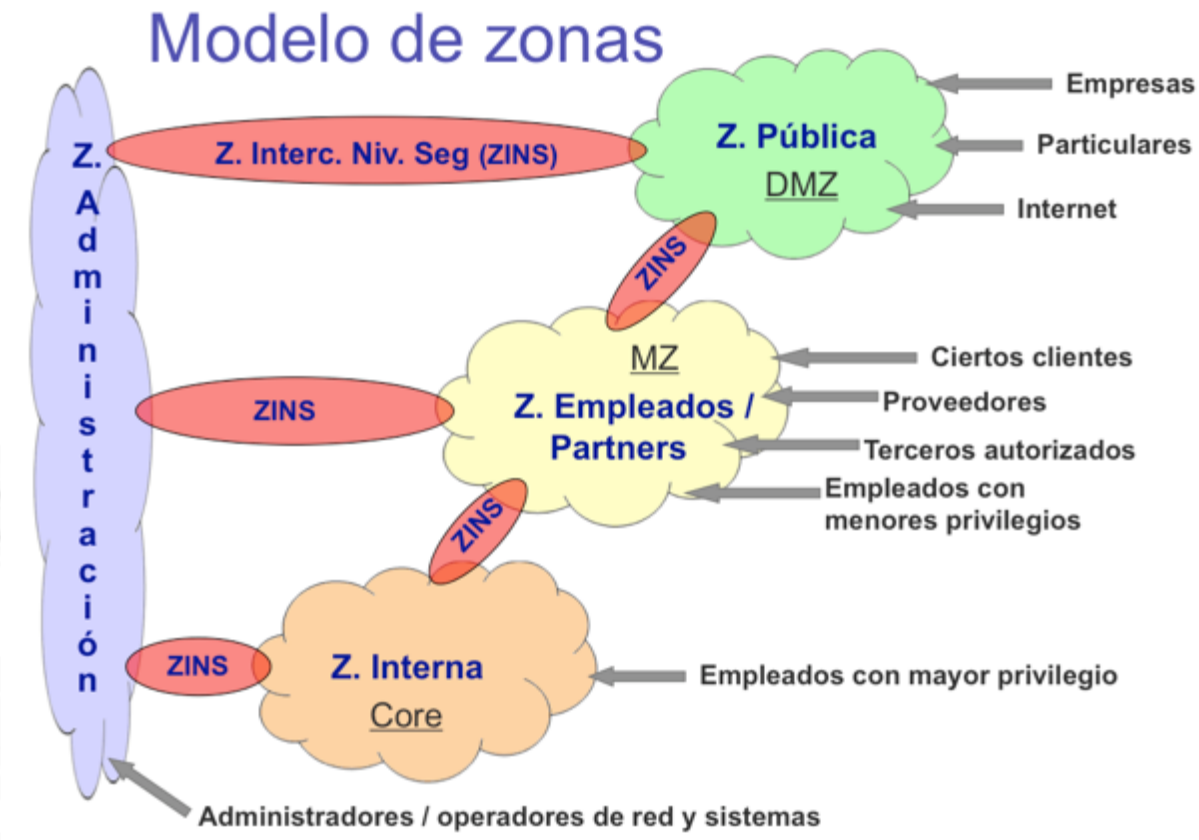


Imagen modelo de zonas y gestión de accesos

A medida que nuestra infraestructura va creciendo y avanzando en su ciclo de vida, como es normal en todo sistema, comienza a degradarse, desde el punto de vista de seguridad esto es sumamente peligros pues estaremos ofreciendo cada vez más "flancos" o puntos débiles.

Un concepto interesante a tener en cuenta es el de "**Reducir la superficie de ataque**".

Este concepto que nos parece natural, es antiquísimo, es lo que hacían las legiones romanas con su formación en "tortuga", compactando la formación y protegiendo con sus escudos cuadrados el frente, flancos, retaguardia y altura como si fuera una caja rectangular que avanzaba inmune a lanzas y flechas. Es lo que se hacía en los castillos medievales, cerrando su perímetro, sin dejar aberturas innecesarias. Es lo que haríamos en cualquier casa cuando salimos de vacaciones.

Para nuestras infraestructuras, implica no ofrecer servicios innecesarios, cerrar o deshabilitar puertos y protocolos que no se usan, "homogeneizar" plataformas, SSOO, servicios y aplicaciones. No dejar configuraciones por defecto o temporales, limitar accesos a que los necesite, mantener una buena política de borrado y modificación de usuarios y privilegios, Evitar obsolescencia de hardware y/o software. No emplear protocolos inseguros, mantener una seria política de parcheado y actualizaciones, concienciar al personal, etc.

Podemos representar estos conceptos como se puede ver a continuación.

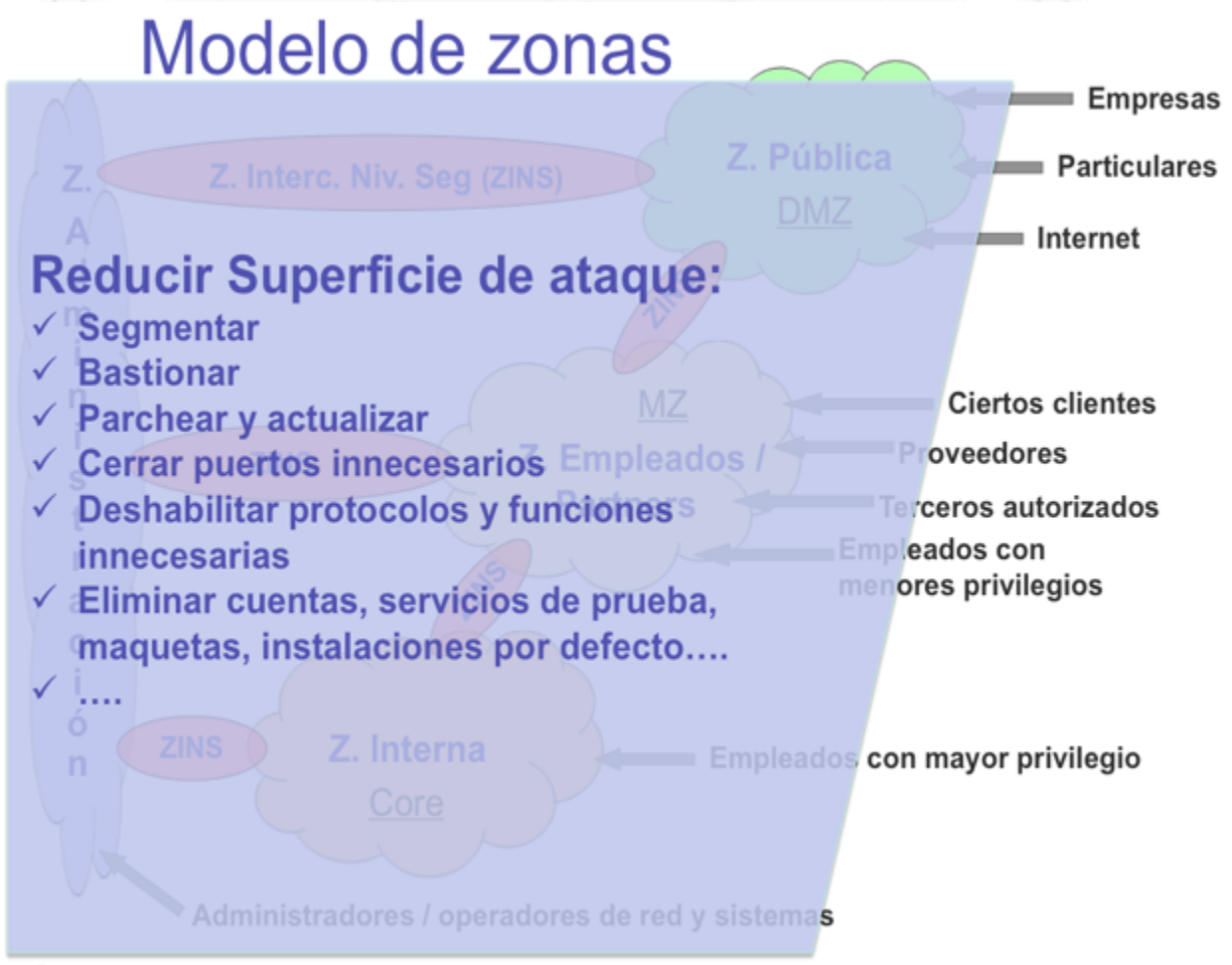


Imagen reducción superficie de ataque

7.4. Nuevos desafíos.

Todo este conjunto de medidas que venimos describiendo, nos obligan a ser "proactivos", a innovar día a día en nuestro trabajo, a investigar novedades que aparecen en la red.

En esta sección vamos a presentar algunas medidas técnicas que nos ofrece la tecnología actual, las cuáles pueden mejorar substancialmente nuestra arquitectura de ciberseguridad.

7.4.1. Protocolo 802.1x

El resumen de este protocolo, podríamos definirlo como: Autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto. Es utilizado en algunos puntos de acceso inalámbricos cerrados y se basa en el protocolo de autenticación extensible (EAP) que regula la **RFC 3748**.

802.1x es una norma para incrementar el control de accesos. Básicamente propone un dispositivo que hace las veces de "puerta de acceso" que por defecto está siempre cerrada, al hacerse presente un elemento que desea acceder (*suplicante*), el dispositivo que recibe esta petición (y que reiteramos, tiene su puerta cerrada), realiza las veces de "pasarela" enrutando esta petición hacia el dispositivo responsable de la "Autenticación" (LDAP, RADIUS; Kerberos, etc.), el mecanismo o algoritmo de autenticación puede operar de diferentes formas, pero en definitiva, luego del diálogo de autenticación, si la misma es válida, entonces recién allí "abre su puerta" de acceso. Este protocolo puede ser empleado tanto en redes cableadas, como en redes inalámbricas y opera en el nivel 2.

Desde el punto de vista de seguridad de una red LAN, no puede ser dejado de lado, al menos en su análisis y mínima

configuración, y es altamente recomendable su implementación pues hoy en día cualquier switch o punto de acceso programable de gama media ya incorpora este protocolo.

El detalle de este protocolo puede analizarse en el punto 4.2.5. 802.1x Autenticación de dispositivos conectados a un puerto LAN, del libro "**Seguridad en Redes**".

En esta sección, sólo deseamos hacer una representación gráfica del funcionamiento del mismo, y cómo este protocolo puede ser implementado en las diferentes zonas que venimos desarrollando en este libro.

La representación de su funcionamiento queda bastante clara, haciéndolo según la simbología de los circuitos electrónicos, en los cuáles, un "conmutador" (*es decir la tecla que presionamos en casa para encender una luz*) es una llave de paso "Normal Abierta" que al ser presionada cierra ese circuito permitiendo el paso de la corriente eléctrica. En nuestro caso, tal cual lo venimos describiendo el protocolo 802.1x funciona de forma similar en su lógica.

La imagen que sigue podemos ver representado este modelo de circuitos sobre las diferentes zonas de nuestra arquitectura propuesta.

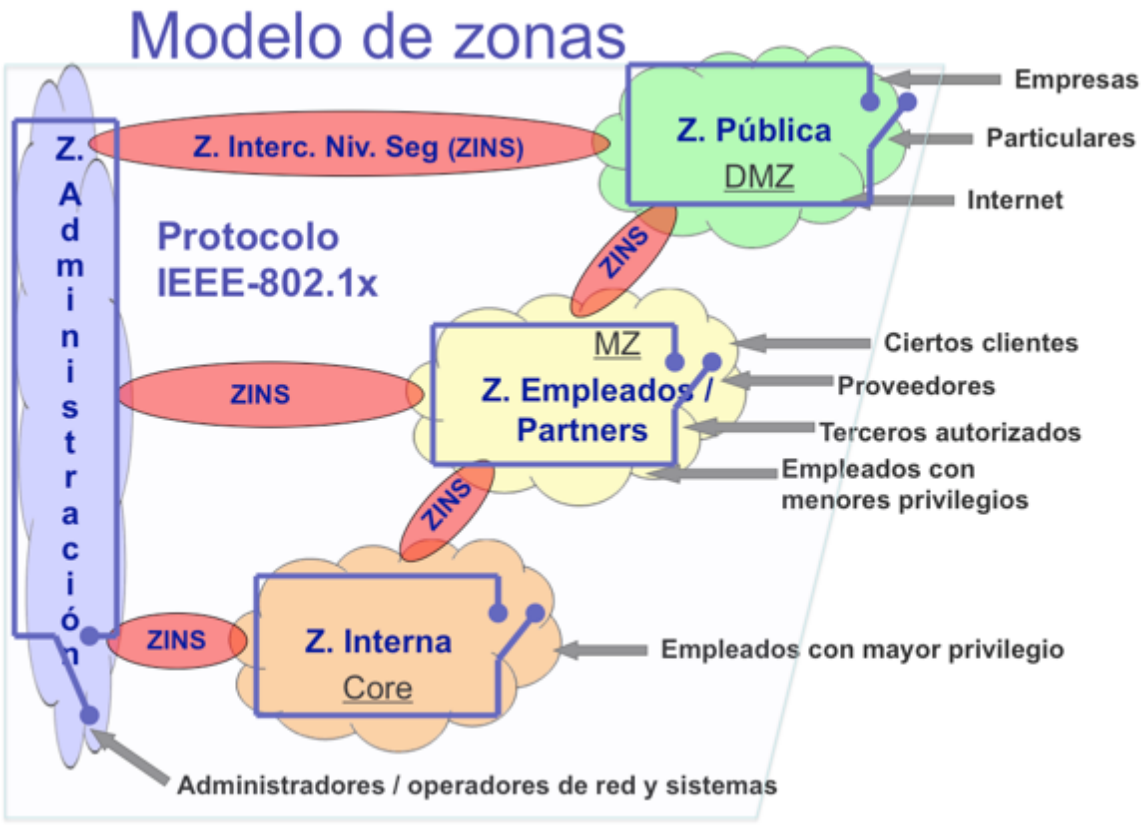


Imagen representación del protocolo 802.1x

*7.4.2. **Protocolo 802.1Q** (Virtual LAN).*

Este protocolo es el empleado justamente para la creación de **VLANs** dentro de un mismo switch y poder separar diferentes "dominios de colisión" bajo el concepto de "Trunking", lo veremos con mucha frecuencia y desde el punto de vista de la seguridad merece la pena prestarle atención pues un uso inadecuado, es foco importante de problemas.

802.1Q permite la creación de VLANs, agregando un encabezado de 4 bytes dentro de la misma trama Ethernet. Para que un Switch "encapsule 802.1q" debe tener configurada sus interfaces y sus VLAN para ello. Las buenas prácticas, nos indican que si tenemos más de un switch, es mejor hacerlo bajo la idea de Interfaces "Trunk" (o troncal), que no son otra cosa que enlaces físicos entre los dispositivos (*generalmente Switchs, aunque no*

exclusivo de estos) por los cuales "entroncaremos" (*aunque suene feo…)* varias VLAN, transportando el tráfico de varias de estas a la vez creando una especie de jerarquía entre ellos. Existe una VLAN por defecto que es la VLAN 1 (*o VLAN nativa*), la cual, ante cualquier error, omisión o ausencia de configuración, será por la que el switch envía toda trama y sin agregar ningún encabezado 802.1Q, por esta razón es que esta VLAN 1 SIEMRE debe estar deshabilitada como medida de seguridad, debiendo tener precaución (*en cuanto a switching*) de cómo opero o creo esta ruta por defecto o nativa en mi switch. Por supuesto que cada VLAN que es configurada en un extremo de cada Trunk debe ser idéntica en el otro pues en definitiva se trata de una conexión punto a punto.

¿Por qué es importante considerar la aplicación de 802.1Q?

Como veremos en la imagen siguiente, la primera ventaja es poder identificar: áreas, zonas geográficas, grupos de trabajo, tecnologías diferentes, etc.

En segundo lugar, a medida que vayamos avanzando en este capítulo, podremos comprobar que todo este conjunto de medidas, aplicadas de forma "Organizada y Coherente" conllevan a concatenar barreras de seguridad que en su conjunto nos ofrecerán un valor agregado substancial y muy diferenciativo a que si cada una de las mismas se adoptaran o analizaran individualmente.

Para ampliar más aún sobre este protocolo, os recomendamos la lectura del punto 4.2.3. 802.1Q (Virtual LAN) del libro "**Seguridad en Redes**".

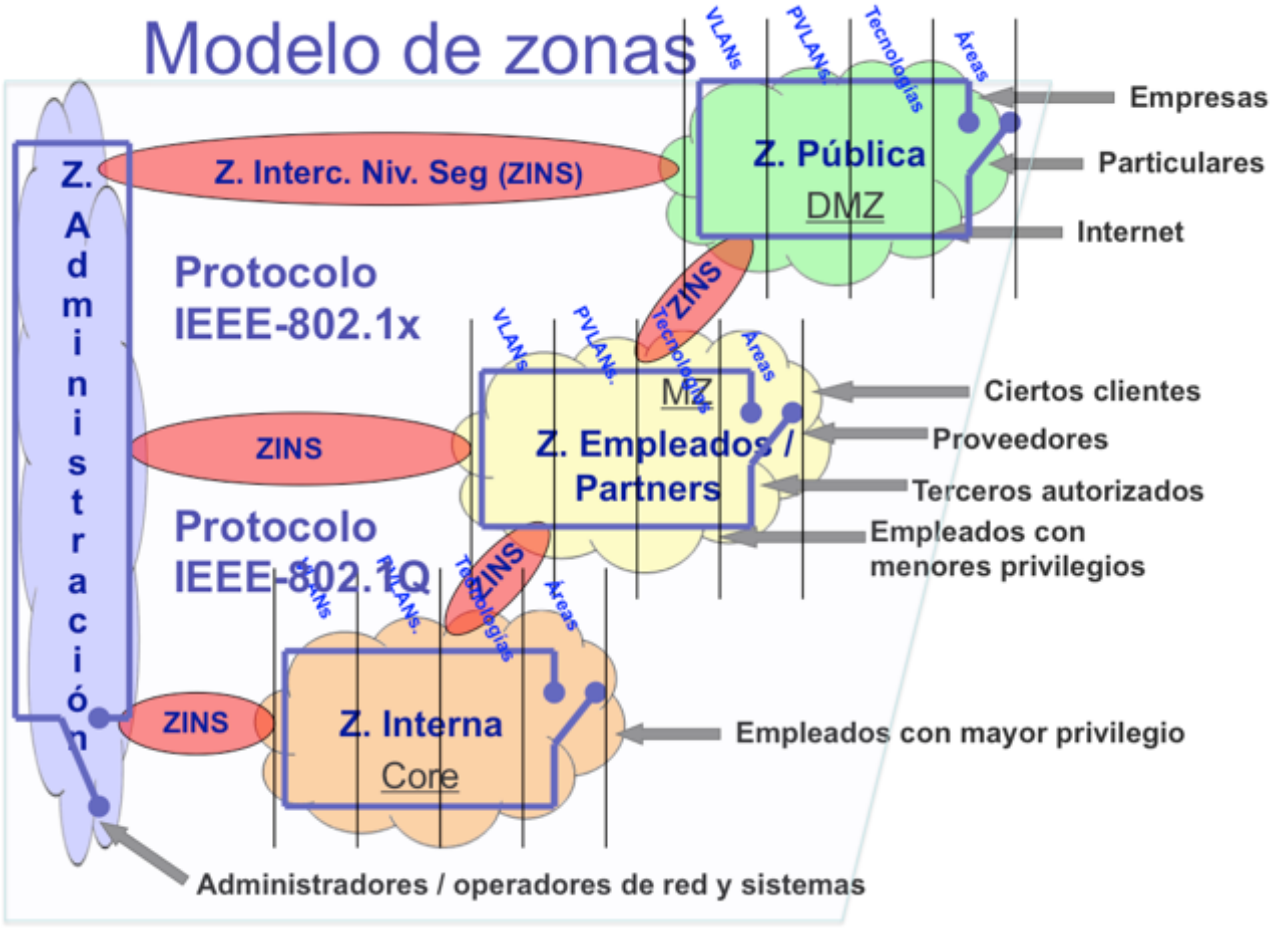


Imagen representación del protocolo 802.1Q

Para comenzar a "Concatenar" medidas de seguridad, presentamos a continuación una imagen, en la cual solamente ampliamos una de estas zonas. En este ejemplo la presentamos como la Red de Gestión de esa zona y hemos elegido el rango privado 10.x.x.x.

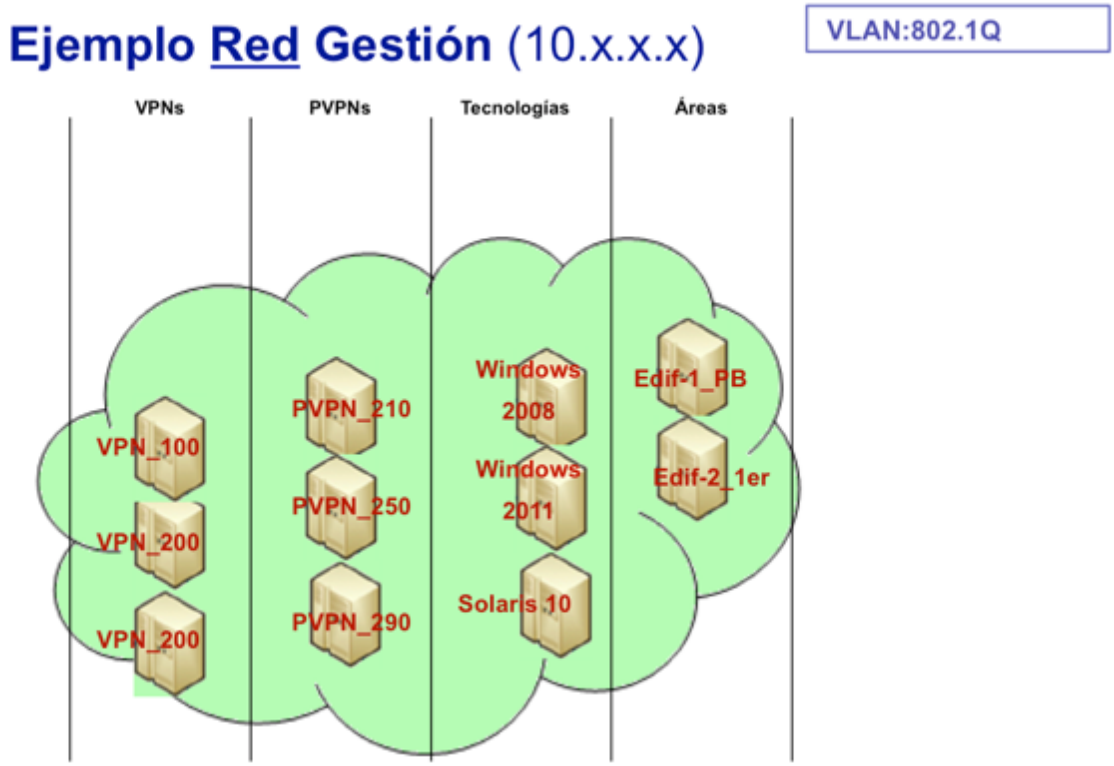


Imagen ejemplo de una red de gestión 10.x.x.x

7.4.3. Segmentación a nivel 3

Una de las principales medidas que podemos emplear a nivel de red, es la "Segmentación" de redes, empleando justamente el concepto de máscara de red y/o máscara de subred. Para ampliar sobre estos conceptos, recomendamos la lectura del capítulo 5. El nivel de Red, el libro "**Seguridad por Niveles**".

Una vez que hemos implementado una buena (*y lógica*) política de segmentación a nivel direccionamiento IP, podemos avanzar tranquilamente al control de rutas y de reglas de control de acceso. Todo aquello que no "enrutemos" concretamente entre esos segmentos de red, no será alcanzable a través de los diferentes segmentos de nivel 3, por lo tanto, si alguien logra comprometer un dispositivo en uno de estos segmentos, y las reglas que hemos puesto en nuestras "Zonas de Intercambio de Niveles de Seguridad" son adecuadas, este intruso solamente

podrá navegar en ese segmento, pues no tendrá acceso, ni siquiera enrutamiento a ninguna otra. En la siguiente imagen, podemos ver un ejemplo sencillo de cómo hemos segmentado esa zona en cuatro rangos diferentes de subredes, y concretamente, si no se establecen rutas o permisos en el Firewall que vemos en la parte superior (*y regula nuestra ZINS*), ningún dispositivo podría llegar a otro segmento.

Como detalle adicional, en esta gráfica vemos también como a su vez estamos empleando 802.1Q para crear VLANs dentro de estos segmentos de red y también para seguir avanzando en el tema, hemos definido algunas tecnologías y áreas diferentes (*Windows, Solaris, Edificio-1 PB, Edificio2 primer piso).*

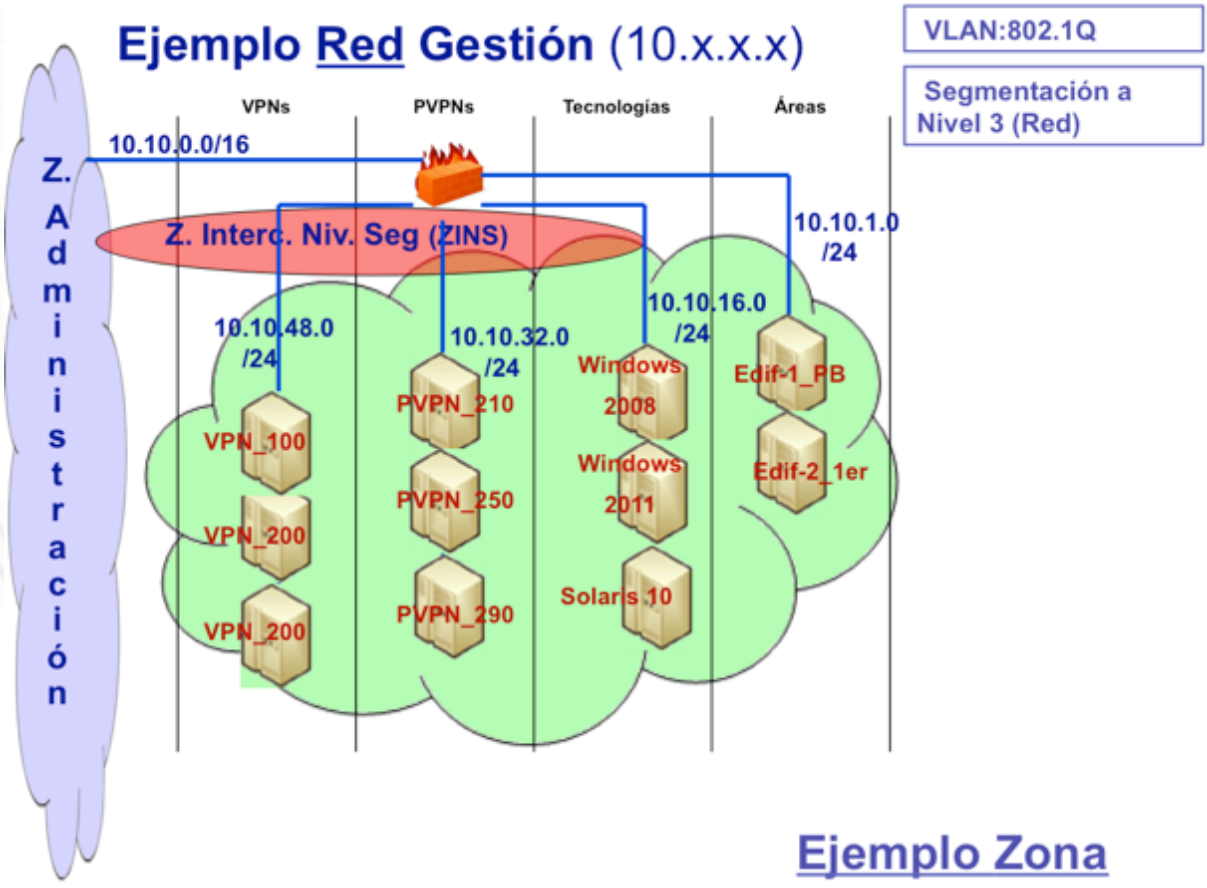


Imagen ejemplo de una red segmentada y de VLANs

Sobre esta misma imagen, superpongamos ahora el empleo de 802.1x. Podríamos representarlo de acuerdo a la siguiente imagen.

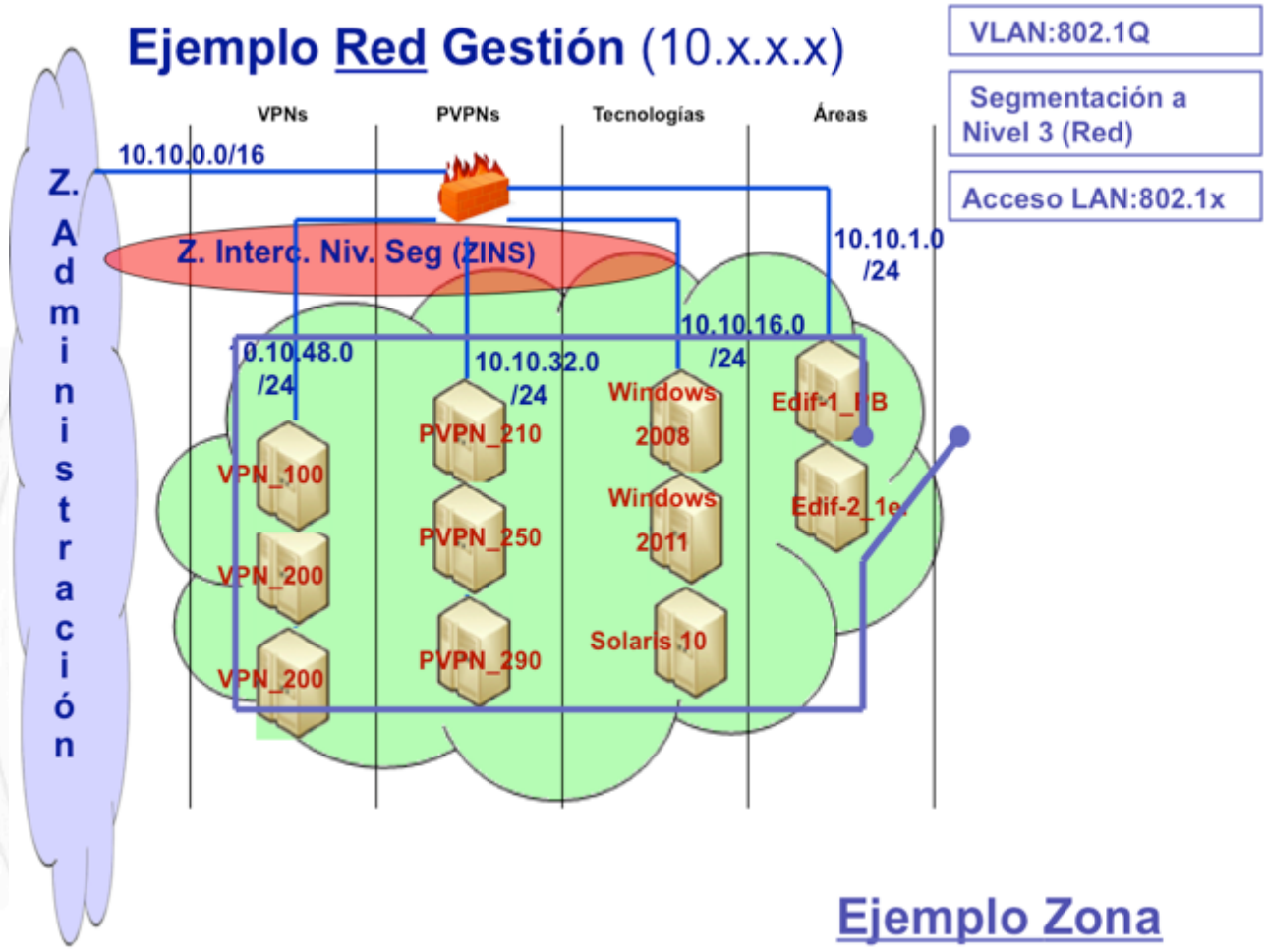


Imagen ejemplo de una red segmentada, 802.1Q y 802.1x

7.4.4. Seguridad en WiFi

Hoy en día, podríamos afirmar que toda infraestructura de red tiene habilitado algún tipo de acceso WiFi, es prácticamente una necesidad más del mercado.

Siguiendo con esta secuencia gráfica de medidas de seguridad que podemos adoptar, en redes Wifi, lo primero a considerar es la "**Segmentación**". JAMÁS permitamos que una red de invitados (*o guest),* pueda tener algún tipo de visibilidad con nuestra red corporativa (ni de servicios, ni mucho menos de gestión). El resto de las medidas de seguridad, siguen en la línea que estamos presentando, pues todo punto de acceso wifi de empleo profesional (no así los domiciliarios), permiten incorporar 802.1x y 802.1Q.

¿Qué me aporta esto último?

Justamente, concatenando estas medidas de seguridad podemos lograr que cuando alguien, se hace presente en el punto de acceso WiFi, el protocolo **802.1x** lo mantenga fuera de la red hasta tanto valide contra nuestra plataforma de Autenticación y control de accesos (*TACACS, Kerberos, LDAP, etc.)* si este usuario está dado de alta o no. En caso de estarlo, si continuamos concatenando medidas de seguridad, puede también verificar su rol, perfil o grupo y a través de **802.1Q** asignarle una VLAN determinada para ese perfil en concreto, por lo tanto, dependiendo del usuario que se haga presente, logrará un determinado tipo de accesos en base a los permisos que tenga configurado.

Todos los conceptos de seguridad en WiFi están desarrollados en el estándar **802.11i**, cuyo objetivo es la seguridad WiFi.

Tal cual venimos describiendo, este estándar abarca los protocolos **802.1x**, **TKIP** (Temporal Key Integrity Protocol), y **AES** (Advanced Encryption Standard). Cada uno de ellos nos propone poder ofrecer un nivel de seguridad igual a una red cableada, en la actualidad sólo si se implementa a través del algoritmo **WPA2** (*Wifi Protected Access versión 2*).

Para ampliar más sobre el tema podemos consultar en el punto 2.4. Operación de la Seguridad del libro "**Seguridad en Redes**" o en el punto 4.2.1. WiFi (Wireless Fidelity) del libro "**Seguridad por Niveles**".

A continuación, presentamos una imagen donde se aprecia un punto de acceso WiFi y un recuadro poniendo de manifiesto esta necesidad (*hasta podríamos decir "obligación"*) de emplear **802.11i**.

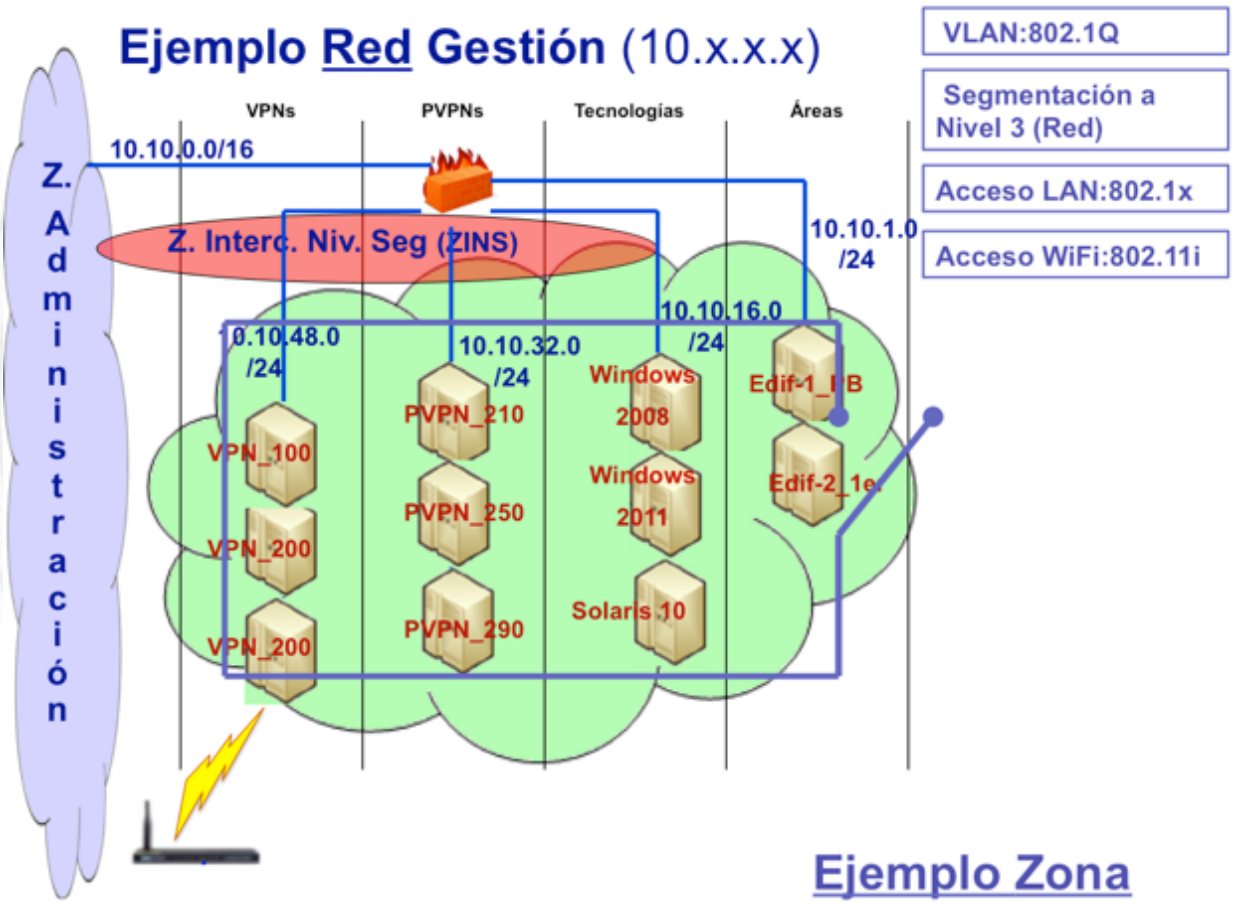


Imagen ejemplo de una red segmentada, 802.1Q, 802.1x y 802.11i

7.4.5. Protocolos 802.1ae y 802.1.af

Estos protocolos ya fueron tratados brevemente en el punto 7.3. Tema base de hoy de **este libro**. Volvamos a la imagen que presentamos allí.

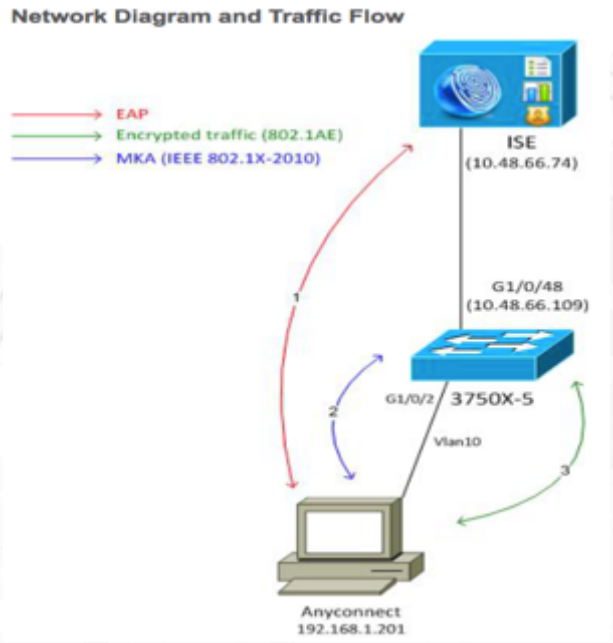


Imagen (Combinación de 802.1x con 802.1ae)

Tal cual desarrollamos en el punto mencionado (**7.3.**), el protocolo **802.1ae** "Media Access Control (MAC) Security", publicado en 2006 y cuya última enmienda es del 2013: 802.1AEbw) es conocido como **MACSec** ofrece confidencialidad, integridad y autenticación de origen, introduciendo nuevos campos a la trama Ethernet.

MACsec crea una "asociación de Seguridad" entre los extremos de ese nivel de enlace, criptografiando todas las tramas en un esquema "Point to Point Encryption".

Las tramas a nivel enlace, se cifran entre el switch y el ordenador que configuren este protocolo. Si se desea que las tramas también se transmitan cifradas entre switchs, puede hacerse configurando también 802.1ae entre ambos switchs.

No es motivo de este punto reiterar conceptos, solamente deseamos seguir "sumando" medidas de seguridad en esta

secuencia que venimos presentando gráficamente, así que a continuación presentamos una nueva imagen donde se puede apreciar un ejemplo de un área que se ha designado como de "máxima seguridad" y sobre la cuál específicamente se aplican estos protocolos.

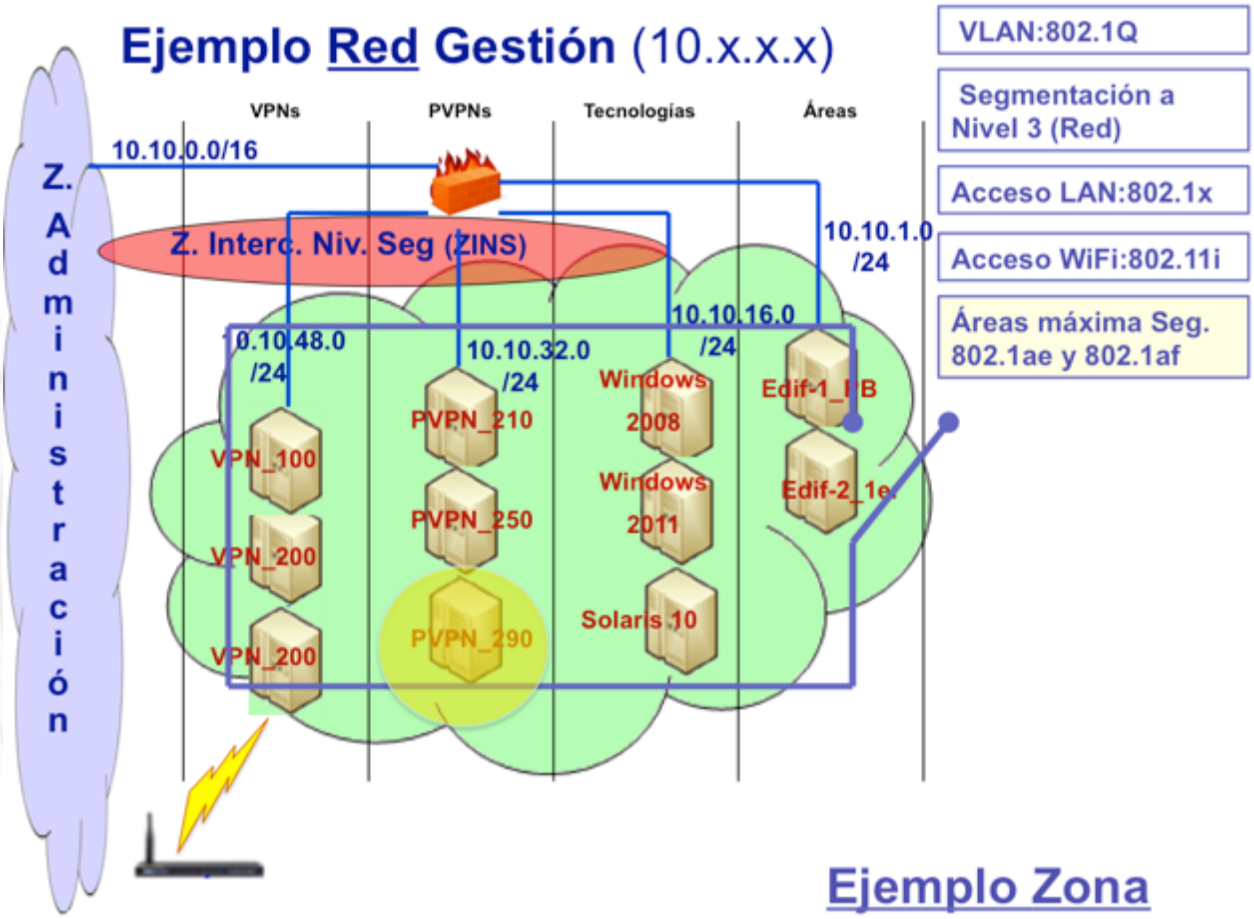


Imagen ejemplo de una red segmentada, 802.1Q, 802.1x, 802.11i, 802.1ae y 802.1af

7.4.6. Protocolo 802.1D (STP) y 802.1aq (SPB)

Uno de los peores problemas que puede presentarse para un Switch es cuando escucha la misma dirección **MAC** (*Medium Access Control*) por dos interfaces físicas diferentes, este es un

bucle que, en principio, no sabría cómo resolver. Este problema si bien parece poco probable que pueda ocurrir, en realidad en redes grandes al tener cientos o miles de cables (*muchos de ellos para redundancia*), este hecho es tan sencillo como conectar el mismo cable en diferentes patch pannels que cierran un lazo sobre el mismo dispositivo, y en la realidad ocurre con cierta frecuencia, mayor, en la medida que más grande sea la red LAN. También es un hecho concreto cuando el cableado se diseña para poseer caminos redundantes, justamente para incrementar la disponibilidad de la red.

Cuando físicamente se cierra un bucle, la topología pura de red "Jerárquica" deja de serlo y se convierte en una red "Malla". Para tratar este problema el protocolo Spanning Tree (**802.1D**) crea una red "Jerárquica lógica (*árbol Lógico*)" sobre esta red "Malla Física". Este protocolo crea "Puentes" (bridges) de unión sobre estos enlaces y define a través de diferentes algoritmos que se pueden configurar.

Para ampliar más este tema, aconsejamos ver el punto 4.2.1. 802.1D (Spanning Tree Protocol: STP) del libro "**Seguridad en Redes**".

El protocolo **802.1aq** (***SPB**: Shortest Path Bridging*) aparece en al año 2006, si bien es alrededor del año 2012 cuando se difunde todo su desarrollo completo. La principal característica que ofrece SPB es que permite mantener "activos" todos los enlaces redundantes, sin necesidad de deshabilitar los bucles físicos (*como hace STP*), manteniendo una real topología de "Malla", con ello mejora la eficiencia y los tiempos de convergencia de la red.

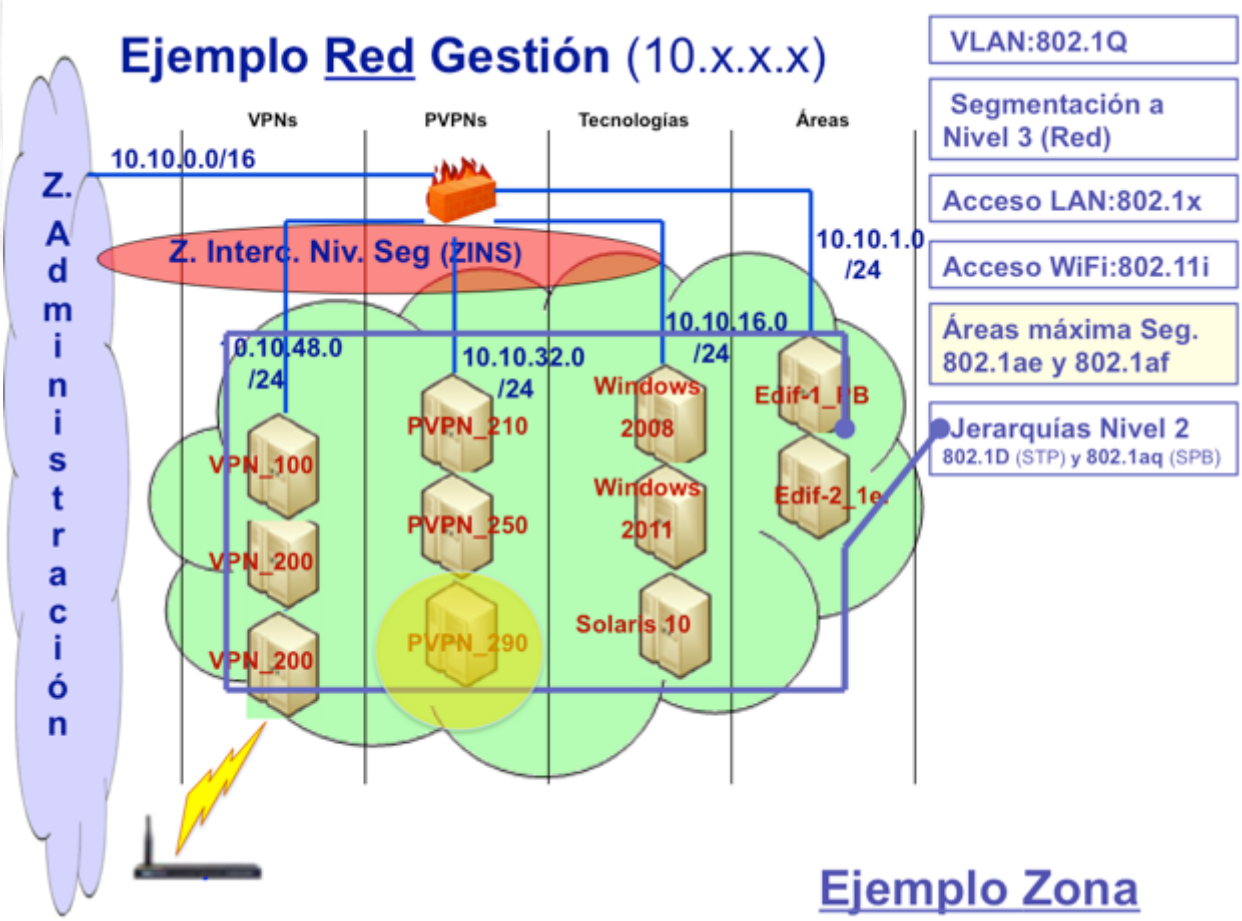
Para ampliar más este tema, aconsejamos ver el punto 4.2.2 802.aq Shortest Path Bridging (SPB) de libro "**Seguridad en Redes**".

Uno de los ataques más sencillos de realizar sobre redes LAN es la falsificación de direcciones MAC. A través de este ataque, se

pueden obtener diferentes tipos de objetivos (*a cuál más peligroso*), desde sencillamente realizar "MAC spoof", hasta aprovechas la misma para realizar "ataques del hombre del medio", realizar escuchas e inyección de tráfico sobre otros dominios de colisión (*es decir otros segmentos del Switch*), escuchar, interceptar y generar tráfico de **VOiP** (*Voz sobre IP*), hasta varios métodos de negación de Servicio.

También existen anomalías de red muy habituales a nivel enlace, que no son provocadas intencionalmente, sino que son fallos de hardware, software o humanos.

Para evitar (*o al menos minimizar el impacto*) todo este tipo de inconvenientes, es que se han diseñado estos protocolos. En la imagen que sigue, presentamos también a estos como otra medida para seguir "concatenando" acciones desde el punto de vista de la seguridad.



7.4.7. Virtualización de host

La tecnología de virtualización ha avanzado de forma exponencial en los últimos años. Hemos visto aumentar su capacidad de forma inimaginable. Hace unos meses, en la visita a un gran CPD (Centro de Procesamiento de Datos) vimos trabajar en sólo tres racks de comunicaciones, más dos únicamente para almacenamiento, un VMCenter que alojaba cuatro mil servidores virtuales, por supuesto que cualquiera de ellos tenía al menos las mismas prestaciones que si fuera un servidor real (*me atrevería a afirmar que bastante más aún*).

Se trata de estas paradojas de la vida, pues si lo analizamos fríamente, estamos retrocediendo a 40 años atrás como si fueran los viejos "main frames" de arquitectura "maestro – esclavo" pues también los hosts a nivel cliente y sus aplicaciones, hoy en día se están ejecutando de forma virtual en grandes plataformas virtuales….

La virtualización es probable que sea el camino de los próximos años.

Desde el punto de vista de ciberseguridad, es también un aspecto clave, si bien debemos prestar mucha atención a su adecuada configuración y bastionado, también nos ofrece un camino nuevo que como iremos viendo en las próximas líneas puede ser muy ventajoso.

Este concepto es la configuración y el control de "**GRANJAS**".

Lo que proponemos aquí es que desde el o los servidores de virtualización, diseñemos (desde el principio) una filosofía de administración del mismo a través de **GRANJAS de servidores**. Cada granja puede contener una misma tecnología, diferentes versiones de esta tecnología, mismas aplicaciones, funcionalidades, servicios, etc.

Si somos capaces de avanzar en esta línea, iremos centralizando sistemas operativos, versiones, administradores de plataformas, inventariado, obsolescencia, etc. De forma coherente.

Esta medida, en cuanto a ciberseguridad tiene muchas ventajas:

- Control por tecnología, prestación, servicio, modelo.
- Sencillez de procesos de entrada en producción y control de cambios.
- Plantillas de bastionado por granja.
- Centralización de actualizaciones y parcheado.
- Segregación de debilidades.
- Facilidad en los controles de flujo, routing y filtrado.
- Facilidad de Supervisión y monitorización.
- Gran capacidad de resguardo y recuperación.
- Facilidad en redundancia, clusters y disponibilidad del servicio.
- Alta disponibilidad de hardware y software.
- Velocidad en ABM de servicios.
- Ahorro de tiempo y velocidad en tiempos de respuesta.
- Puntos comunes de control (servidores de actualización, parcheado, antivirus, killswitch, etc.)
- "Compartimentación" (*a desarrollar más adelante*).
- Etc.

En la figura que sigue, representamos la capacidad que nos ofrecería la implementación de diferentes tipos de "granjas" a nivel host en nuestro segmento de red.

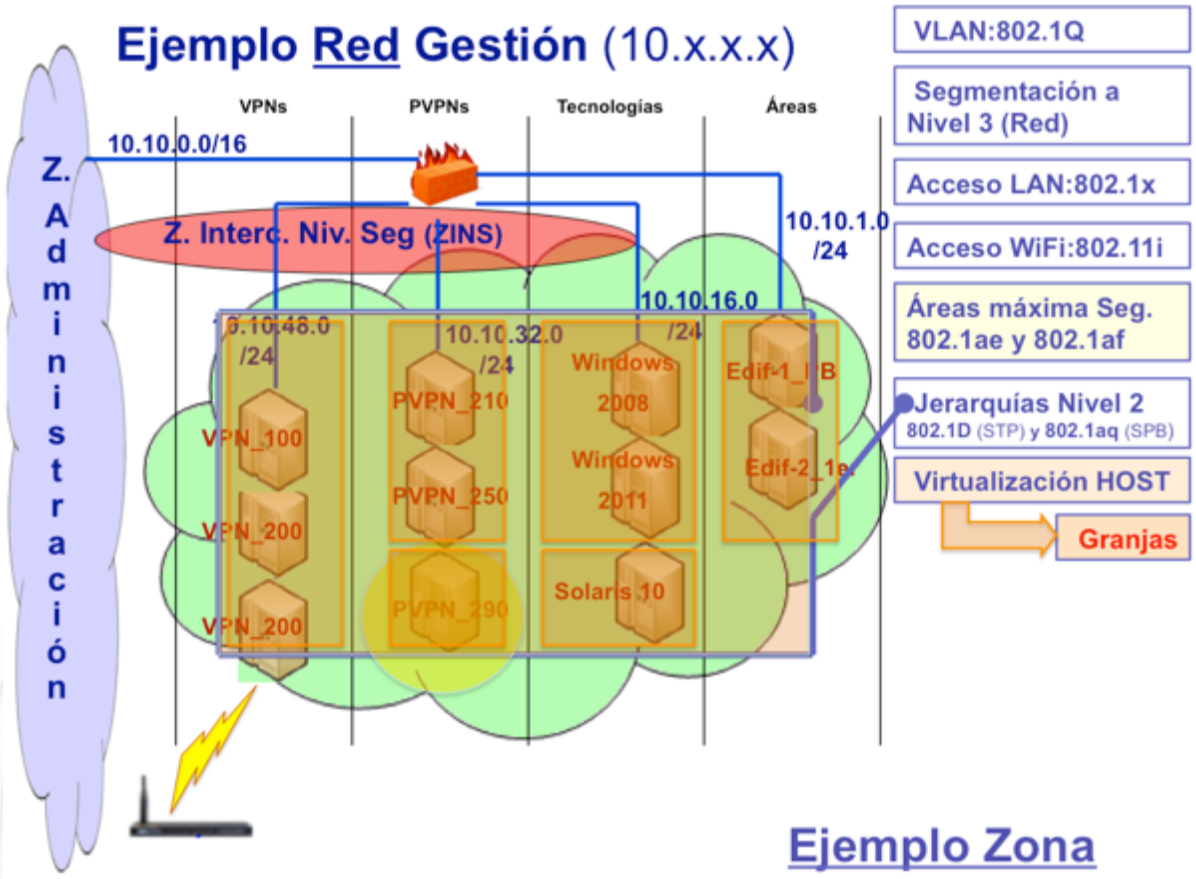


Imagen ejemplo de una red segmentada, 802.1Q, 802.1x, 802.11i, 802.1ae, 802.1af, 802.1D, 802.1aq y virtualización de hosts

7.4.8. "Compartimentación" de red.

Tal vez la ventaja más importante que nos puede ofrecer este último concepto, concatenado con los anteriores, es esta nueva idea que vengo impulsando desde hace meses que la denominé "**Compartimentación de red**".

Este concepto, es fundamental en los tiempos que vivimos.

La idea es que, si hemos llegado hasta este punto, siguiendo el conjunto de medidas de seguridad propuestas, tendríamos una capacidad de gestión de la seguridad con un altísimo nivel de granularidad.

Supongamos (*como viene sucediendo cada vez más a menudo*) que surge un nuevo tipo de malware que ataca a cualquier tipo de tecnología, sistema operativo, versión, etc. (*Recordemos WannaCry o Petya*). Si hemos cumplido con los pasos propuestos, tenemos a nuestra disposición varios cursos de acción, para que solo haciendo un "**click**" podamos **aislar completamente** en target de este ataque, y acotarlo exclusivamente a la zona, área, granja o VPN que queramos.

La idea es diseñar e implantar todo este conjunto de medidas, de la mejor forma que se ajuste a nuestra arquitectura de redes y sistemas. Una vez que tengamos bien encaminada esta fase, dediquemos todo el tiempo que esté a nuestro alcance para:

1) Realizar breves análisis de riesgo de estas zonas.
2) Identificar hipótesis de ataques.
3) Planificar y realizar "juegos de ciberguerra" (sobre estas hipótesis).
4) Reciclar las experiencias de estos ejercicios, mejorando la capacidad de reacción o "resisliencia" de nuestras infraestructuras.

En la imagen que sigue, presentamos gráficamente los conceptos de este punto.

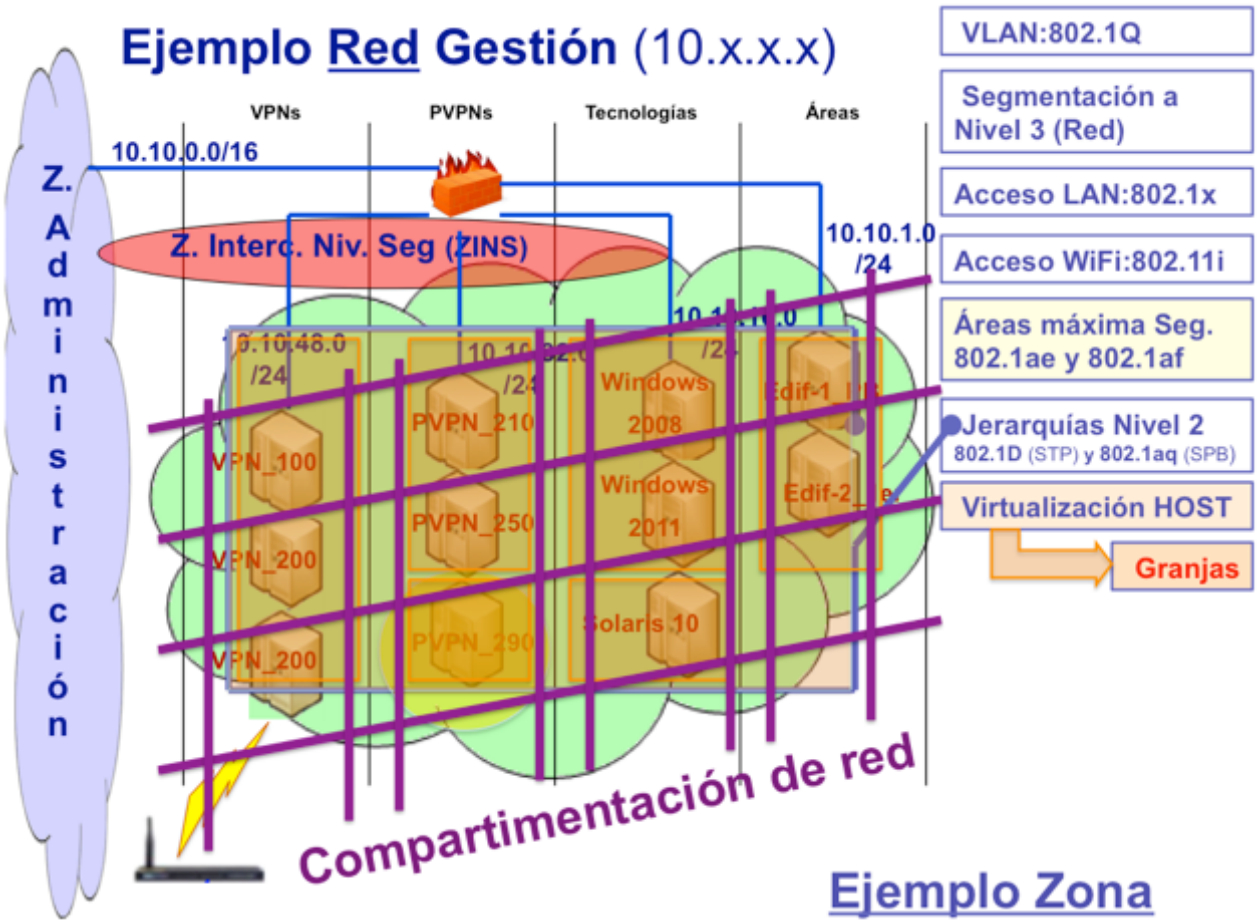


Imagen ejemplo de una red segmentada, 802.1Q, 802.1x, 802.11i, 802.1ae, 802.1af, 802.1D, 802.1aq, virtualización de hosts y "Compartimentación"

7.4.9. Virtualización de red

El último aspecto técnico que desarrollaremos, son las diferentes metodologías que podemos emplear para conectarnos remotamente a nuestras infraestructuras, de forma tal que la conexión sea exactamente igual a la que realizaríamos si estuviéramos sentados frente al dispositivo o en su propia red LAN.

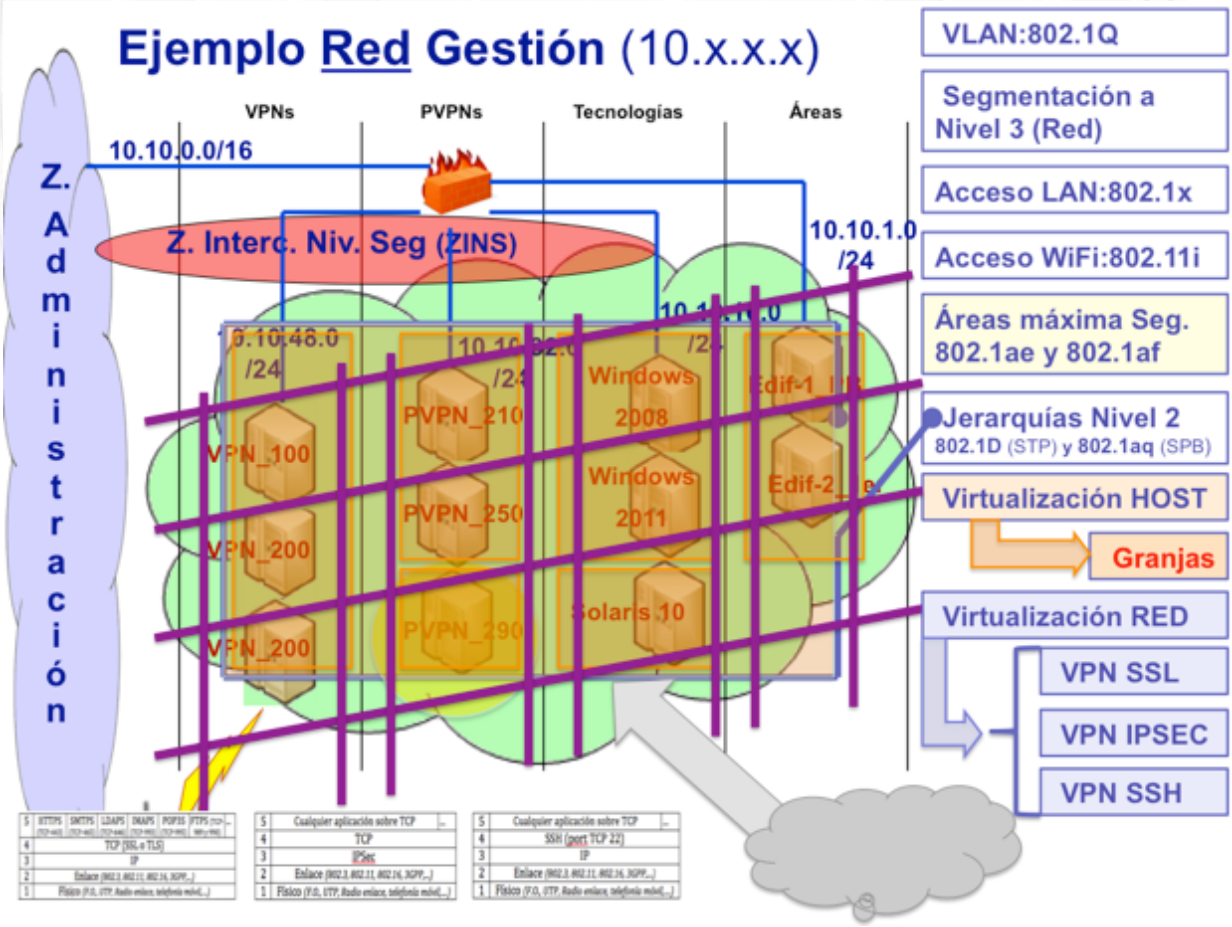
Tal vez esta no sea la definición más escolástica de las redes virtuales, pero es probable que sea la más clara, pues lo que intentaremos detallar a continuación, es precisamente esto, las

técnicas concretas que podemos emplear estando en casa, o en cualquier sitio del mundo para poder trabajar con las mismas funcionalidades y servicios que desde la misma oficina.

Existen varias herramientas comerciales y de open source que ofrecen más o menos amigabilidad o potencia a la hora de cumplir este cometido, pero básicamente todas ellas se basarán en las siguientes técnicas:

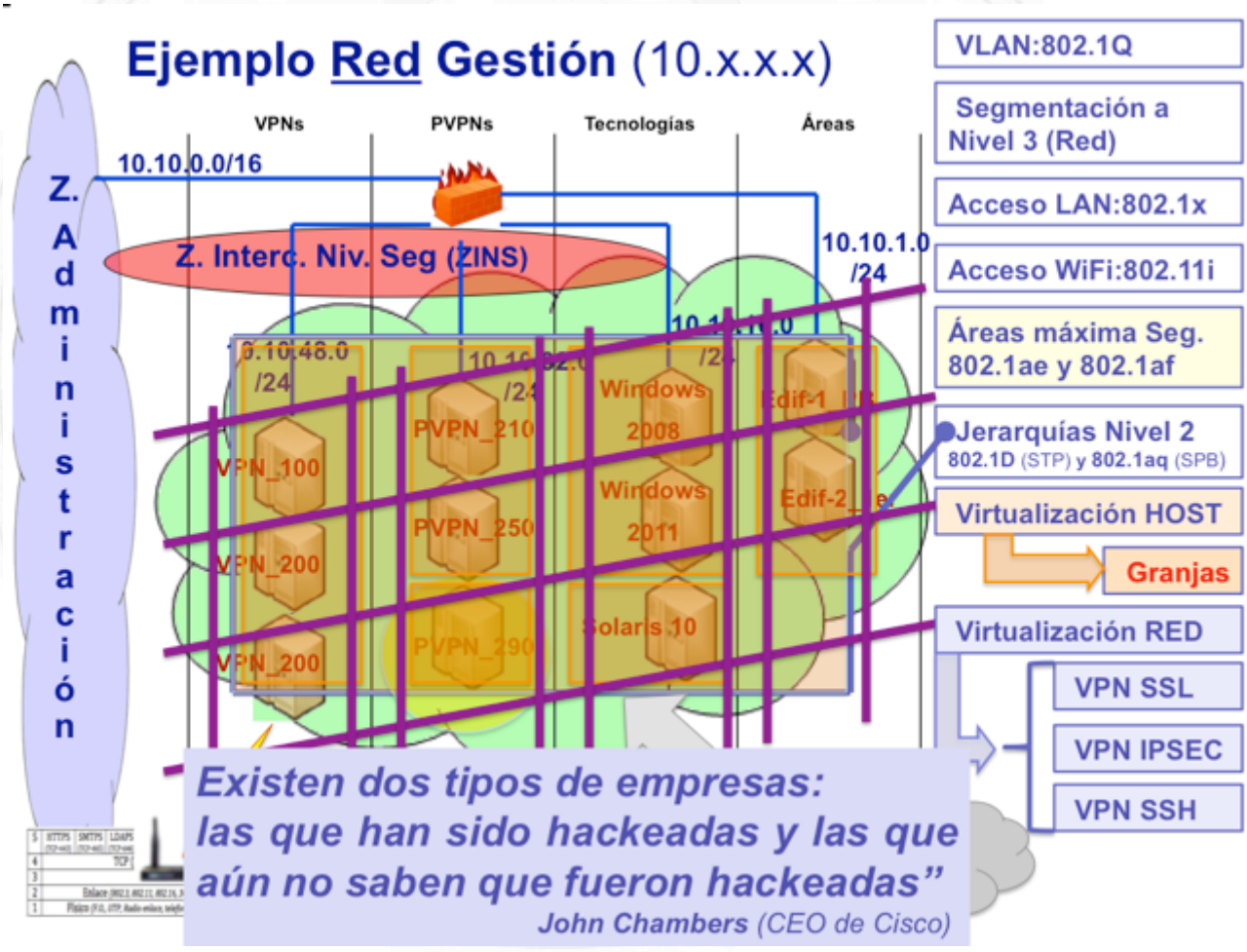
- VPN empleando SSL (*Secure Socket Layer*)
- VPN utilizando IPSec
- VPN a través de SSH (*Secure SHell*)

Este tema ya fue desarrollado con suficiente detalle en el punto 7.3. Tema base de hoy del **presente libro**, por lo tanto no profundizaremos más, sencillamente presentamos la imagen siguiente para cerrar todos estos conceptos.



7.4.10. Resiliencia

Analicemos la siguiente frase.



¿La compartes, o aún te queda alguna duda al respecto)?

Seamos conscientes que nuestras infraestructuras, tarde o temprano sufrirán algún tipo de incidente de seguridad. Dejemos de pensar que somos invencibles pues ese fue el gran error de los grandes imperios o dictadores, tarde o temprano cayeron.

Si somos capaces de enfrentar esta realidad, entonces sigamos adelante mejorando todo este conjunto de medidas que hemos ido presentando y, como último aspecto, reiteremos una vez más lo siguiente:

El conjunto de procedimientos y las adecuadas acciones para su implementación, lo que conlleva todo su "**ciclo de vida**", serán la salvaguarda final que nos permitirá retornar nuestra organización a un estado operativo en el menor tiempo posible.

7.4.11. Ruido de red

El tema final de cierre de este libro, lo desarrollaremos nuevamente con un concepto que propone "Cisco" en su análisis del 2017. Este concepto lo ha titulado "Ruido de Red.

Veamos primero la imagen que presentamos a continuación para poder seguir adelante con este concepto.

Ruido de red:

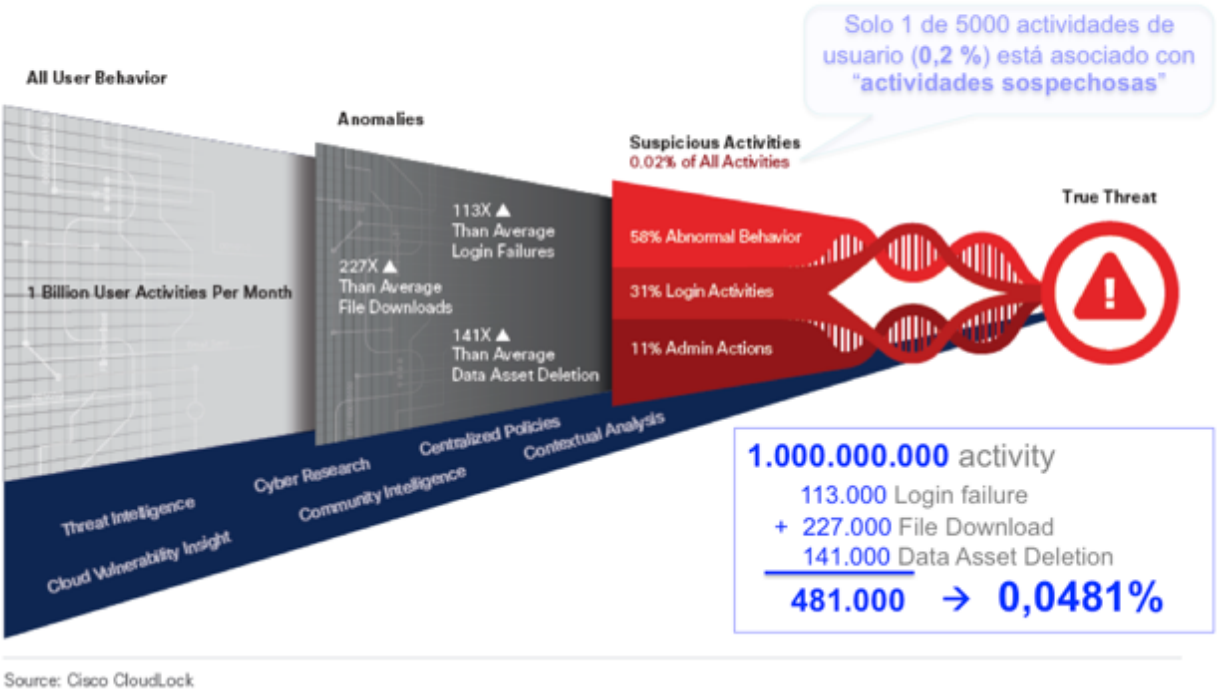


Imagen tomada del "2017 Annual Cibersecurity report" de Cisco

Esta imagen se genera, como se puede apreciar (*en la parte gris clara de la izquierda*), sobre la base de 1.000.0000.000 de actividades de usuarios por mes, es decir podemos considerarlo como una muestra suficientemente significativa en relación a cualquiera de nuestras organizaciones.

En el centro de la imagen (*parte gris oscuro del centro*) se pone de manifiesto que sólo el 0,0481 % de esta actividad pueden ser consideradas "Anomalías" de la red, estas peculiaridades las asocia a Fallos de login, descargas de ficheros y borrado de datos.

Por último, la parte **roja** de la derecha, nos muestra que únicamente 1 de 5000 paquetes se consideran como "**Actividad sospechosa**".

La propuesta de esta imagen es totalmente clara y al igual que cualquier otra señal electromagnética, para su análisis, debemos

obtener una señal de "**calidad**", debemos ser capaces de limpiar este tráfico, eliminando todo el ruido posible. El trabajo de análisis de seguridad se potenciará en gran medida, si somos capaces de "separar la paja del trigo" y quedarnos con los eventos que realmente merecen nuestra atención.

Esta es la idea que Cisco propone como "**Ruido de Red**" y lo hace (*como siempre suele hacerlo*) sustentado en datos reales y con una muestra inmensa que no puede ser refutada.

Este tema lo venimos desarrollando a lo largo de muchos de nuestros textos, pues debemos ajustar reglas, políticas, eliminar falsos positivos, seleccionar los Logs a enviar, generar local rules, que miren específicamente los aspectos que particularizan nuestra infraestructura, esas debilidades que no podemos parchear o actualizar, o restringir. Nuestras infraestructuras son diferentes entre sí y cada una de ellas tiene sus defectos y virtudes, por lo tanto, si somos capaces de ir "eliminando el ruido" de las mismas, podremos realizar un trabajo de seguridad mucho más transparente y eficiente.

Este es el mensaje final de nuestro libro, apliquemos todo el conjunto de medidas que esté a nuestro alcance para que cada mes, año sea un nuevo escalón de ciberseguridad, un verdadero "Ciclo de Vida" o "Sistema de Gestión de la Seguridad de la Información" (***SGSI**, tal cual propone la familia ISO 27000),* seamos capaces de tener una red de "Calidad" pues hemos eliminado en gran parte todo ese ruido innecesario y estamos en capacidad de "escuchar y evaluar" lo importante, para poder obrar en consecuencia.

Un afectuoso saludo.

Madrid, 31 de noviembre de 2017.

Alejandro Corletti Estrada

acorletti@darFe.es