VERDAD, BELLEZA, PROBIDAD

UAT

Secretaría de Administración

Dirección de Tecnologías de la Información

LINEAMIENTOS DE ESQUEMAS DE SEGURIDAD DE LA INFORMACIÓN

1 OBJETIVO

Describir los lineamientos aplicados a la gestión y administración de los equipos de seguridad instalados en la salida a Internet y en algunas sedes de la Universidad Autónoma de Tamaulipas. Los equipos que conforman la red de seguridad, son aquellos que nos permiten proteger de accesos no autorizados en diversos puntos de nuestra infraestructura.

2 ALCANCE

Salida de internet y algunas sedes y departamentos de la Universidad Autónoma de Tamaulipas.

3 ÁMBITO DE APLICACIÓN

La aplicación de lineamientos contenidos en el presente documento, corresponde a los Titulares de las Unidades Administrativas o Áreas Responsables de las TI en las dependencias, así como al personal administrativo cuyas atribuciones o funciones estén relacionadas con la planeación, contratación y administración de bienes y servicios de TI y en la seguridad de la información en la Universidad Autónoma de Tamaulipas.

4 DEFINICIONES, SIGLAS, ACRÓNIMOS

Firewall. Dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Es parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

IPS. Es un software o hardware que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de prevención de intrusos es considerada por algunos como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías de Firewall.

DMZ. Una zona desmilitarizada (por sus siglas en inglés de Demilitarized Zone) o Red Perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que en general las conexiones desde la DMZ solo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectarse con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

Botnet. Es un término que hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El dueño de la botnet puede controlar todas las computadoras o servidores infectados de forma remota y se usan para diversas actividades criminales.

Control de aplicaciones. Es un funcionabilidad con la que cuentan equipos de seguridad permitir o bloquear aplicaciones en una red o redes con acceso a Internet. Proporciona un gran apoyo al equipo de seguridad, ya que permite crear políticas a nivel granular, administrar ancho de banda y accesos por horarios.

Portal Cautivo. Un portal cautivo es un programa o máquina de una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal. El programa intercepta todo el tráfico HTTP hasta que el usuario se autentifica. El portal se encargará de hacer que esta sesión caduque al cabo de un tiempo.

VPN. Una Red Privada Virtual, por sus siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

DHCP. Protocolo de configuración dinámica de host. Es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

VLAN. Es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área.

IPV6. El Internet Protocol versión 6 es una versión del protocolo Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol Versión 4 (IPv4) RFC 791, que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet.

5 MARCO DE REFERENCIA

Estándar	Descripción
NAT	Es un mecanismo utilizado por firewalls y routers para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles
IEEE 802.3ab	1000BASE-T Ethernet de 1 Gbit/s sobre par trenzado no blindado.
ARP	Protocolo de la capa de enlace de datos responsable de encontrar la dirección hardware (MAC) que corresponde a una determinada dirección IP. RFC 826
IEEE 802.1Q	Tecnología a nivel de capa 2 del modelo de referencia OSI que ayuda a optimizar, proteger y segmentar el tráfico de la red.
RFC 2131 - IETF	Protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente.
IPV4	Protocolo de Internet versión 4. Definida en el RFC 791.= IPv4 usa direcciones de 32 bits, limitándola a 232 = 4.294.967.296

Estándar	Descripción
IPV6	Es una versión del protocolo Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol versión 4
IPSEC	Internet Protocol Security es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.
3DES	Triple DES se le llama al algoritmo que hace triple cifrado del DES. También es conocido como TDES o 3DES, fue desarrollado por IBM en 1998.
AES	Advanced Encryption Standard (AES) es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.

6 MODELO ORGANIZACIONAL (GRUPO INTERDISCIPLINARIO)

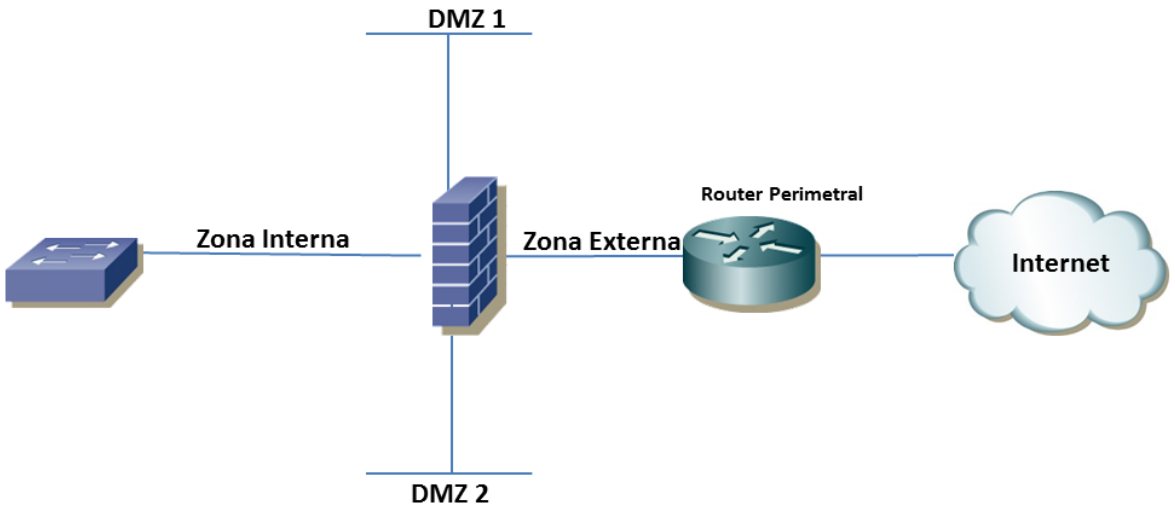
Integración del Grupo de trabajo de Arquitectura Tecnológica.

7 MODELO DE DISEÑO POR ZONAS

El modelo de diseño por zonas tiene como funciones típicas:

- **Zona Interna:** la función principal de esta zona es proteger la red interna de la organización e inspeccionar el tráfico de salida.
- **Zona Externa:** su función es proteger de los accesos no solicitados desde internet, además de publicar servicios que se ofrezcan por parte de la organización donde se encuentra instalado.
- **DMZ:** La función de esta zona es proteger a los equipos de accesos no solicitados, tanto de la zona interna y de la zona externa; además de publicar servicios tanto para la red internet como la zona interna.

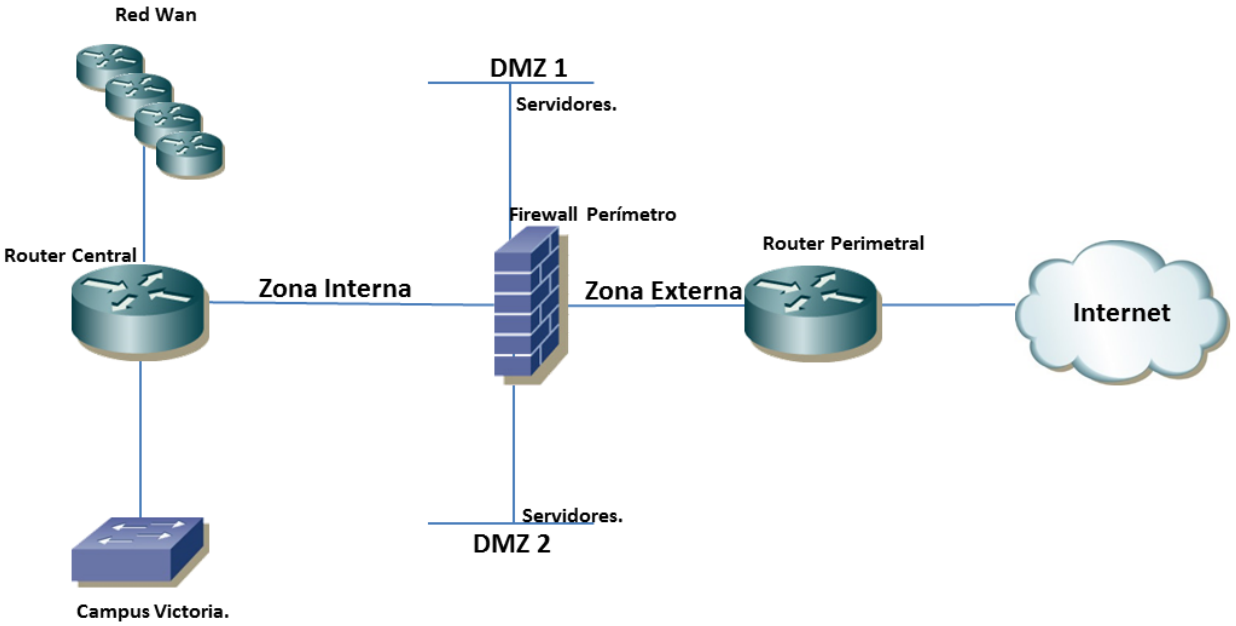
El siguiente diagrama ilustra un ejemplo de la implementación por zonas.



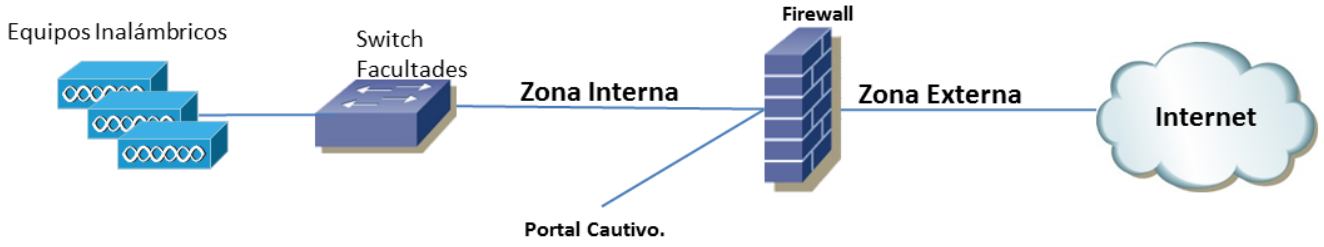
8 ARQUITECTURA TECNOLÓGICA

El modelo por zonas deberá implementarse en la salida a internet y en los departamentos que así lo requieran como se ejemplifica en la salida de internet en el Campus Victoria y en la implementación eUAT.

Implementación de seguridad de Internet Campus Victoria.



Implementación de seguridad eUAT



9 FUNCIONALIDADES

La infraestructura de Seguridad en la Universidad está diseñada bajo el modelo por zonas para ofrecer la seguridad a los diferentes servicios de voz, video y datos, así como la protección de equipos personales de los usuarios conectados a la red universitaria, asegurando una operación confiable y escalable para futuros crecimientos de ancho de banda.

Características de un Firewall:

- Firewall Capa 7.
- Filtrado de URL
- Control de Aplicaciones.
- Control de límite de Ancho de banda.
- Detector de Intrusos. IPS.
- Detección de Antivirus en el Perímetro.
- Anti-botnet
- Funcionabilidad de VPN.
- Reportes y estadísticas de uso.
- Portal Cautivo.
- Análisis de tráfico y eventos.
- Captura de tráfico
- Políticas por tiempo
- Revisión de Antivirus en el perímetro.
- Soporte ipv6
- Servidor DHCP.
- VLAN.
- Soporte de protocolos de Ruteo.