Seguridad en el Router

M. Farias-Elinos

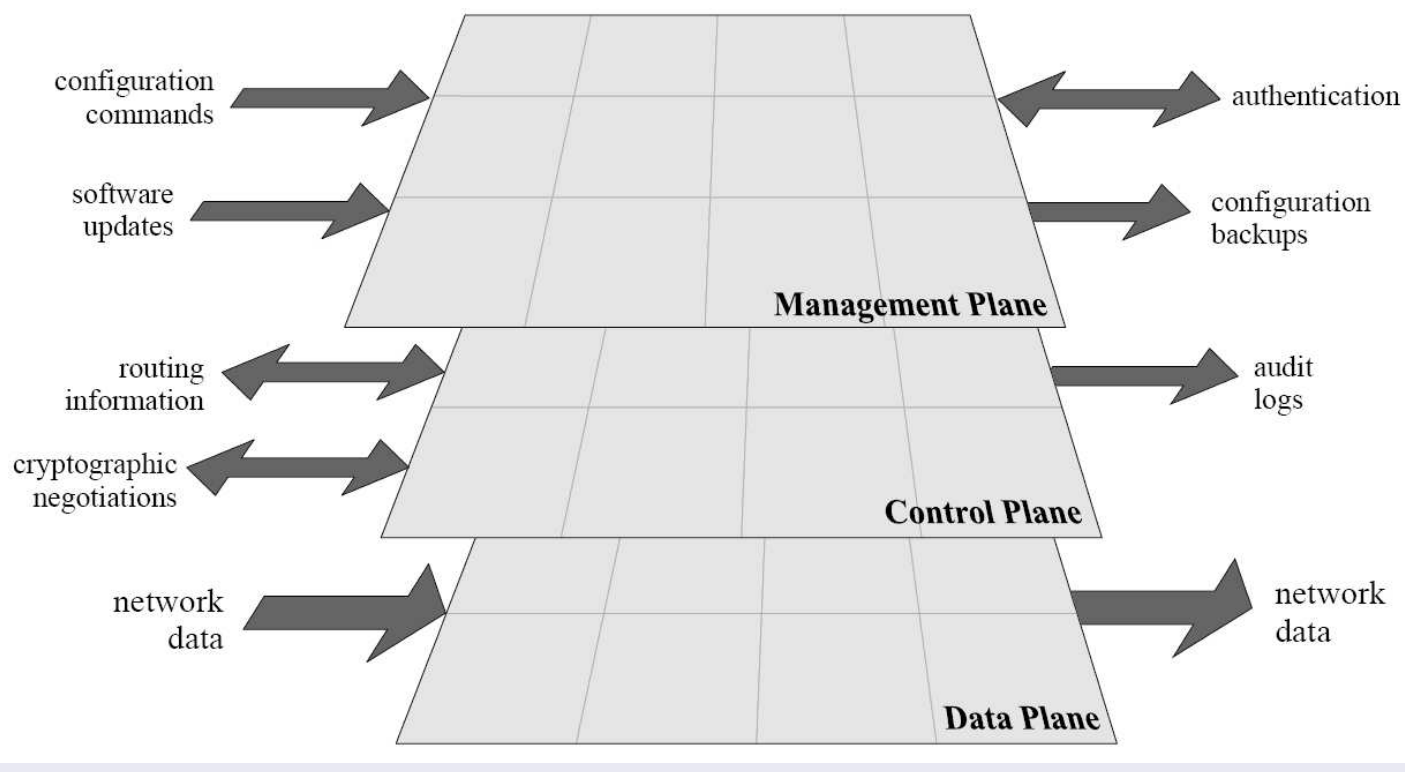
April 16, 2008

1 Introducción a la seguridad del router
- Vulnerabilidades
- Roles del router
- Políticas de seguridad

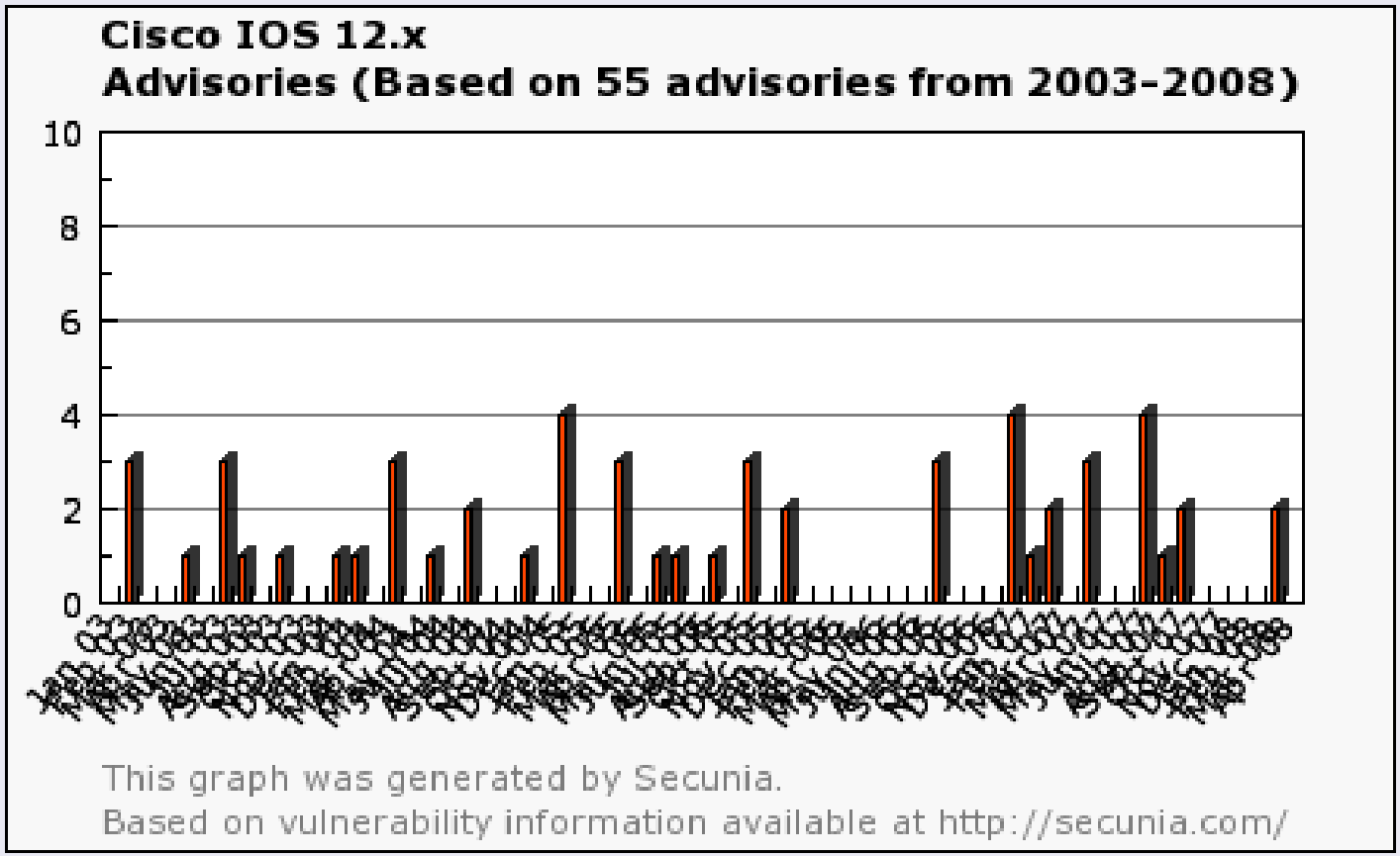
2 Seguridad en Routers

3 Servicios AAA
- TACAS+
- RADIUS

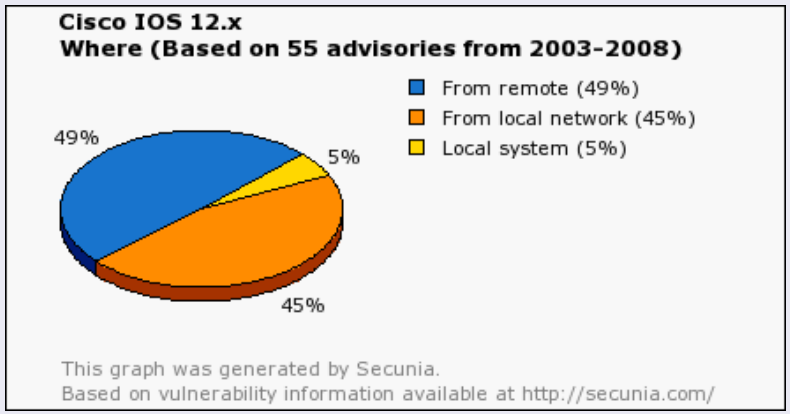
Modelo conceptual del router

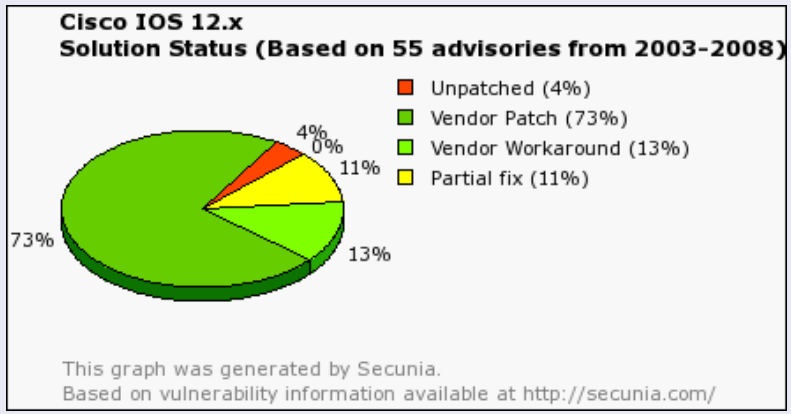


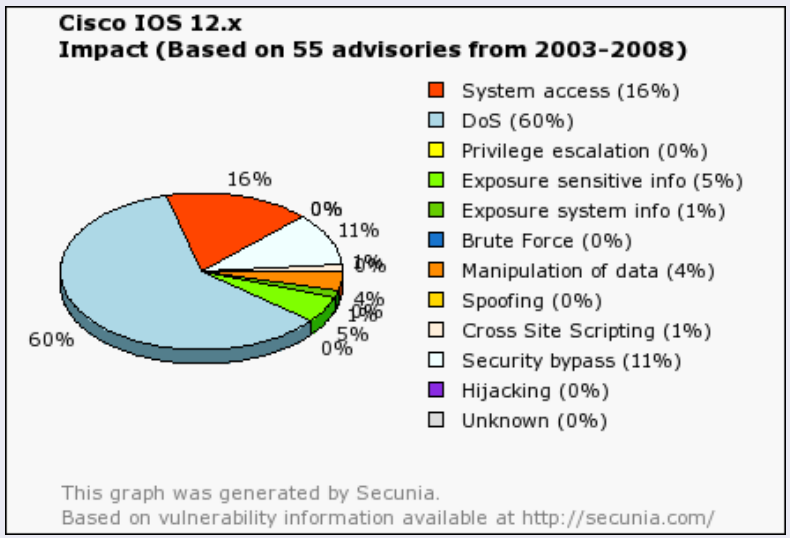
IOS 12


Cisco IOS 12.x
Advisories (Based on 55 advisories from 2003-2008)
10
8
6
4
2
0
This graph was generated by Secunia.
Based on vulnerability information available at http://secunia.com/

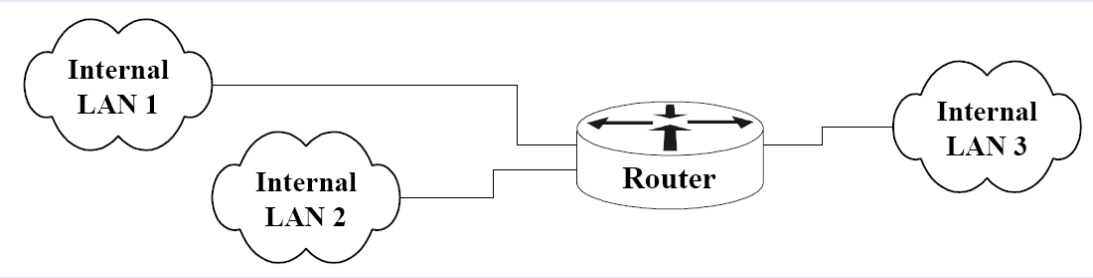
IOS 12


Cisco IOS 12.x
Where (Based on 55 advisories from 2003-2008)
From remote (49%)
From local network (45%)
Local system (5%)
49%
5%
45%
This graph was generated by Secunia.
Based on vulnerability information available at http://secunia.com/

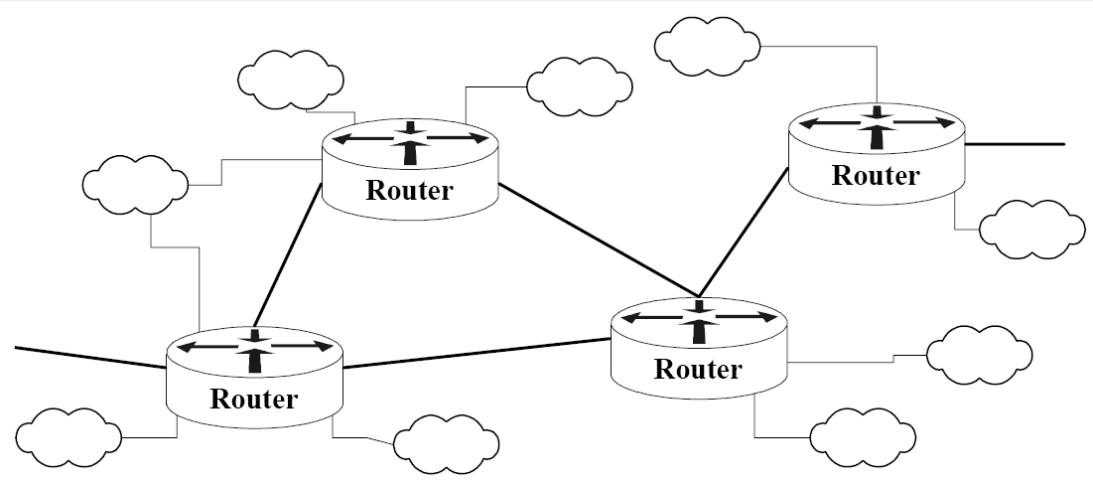

Cisco IOS 12.x
Solution Status (Based on 55 advisories from 2003-2008)
Unpatched (4%)
Vendor Patch (73%)
Vendor Workaround (13%)
Partial fix (11%)
4%
0%
11%
73%
13%
This graph was generated by Secunia.
Based on vulnerability information available at http://secunia.com/


Cisco IOS 12.x
Impact (Based on 55 advisories from 2003-2008)
System access (16%)
DoS (60%)
Privilege escalation (0%)
Exposure sensitive info (5%)
Exposure system info (1%)
Brute Force (0%)
Manipulation of data (4%)
Spoofing (0%)
Cross Site Scripting (1%)
Security bypass (11%)
Hijacking (0%)
Unknown (0%)
16%
0%
11%
4%
5%
60%
This graph was generated by Secunia.
Based on vulnerability information available at http://secunia.com/

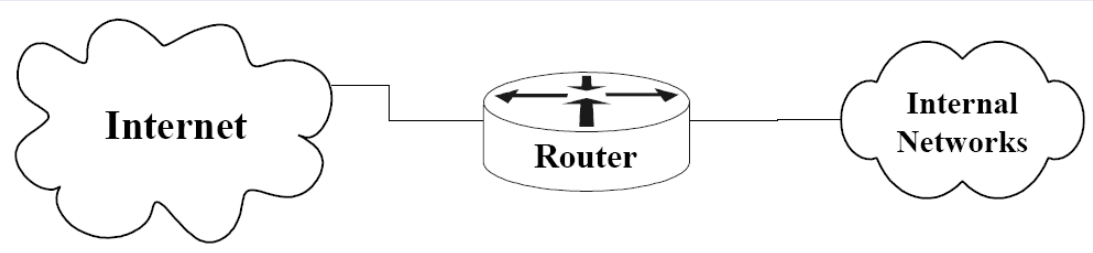
Interiores



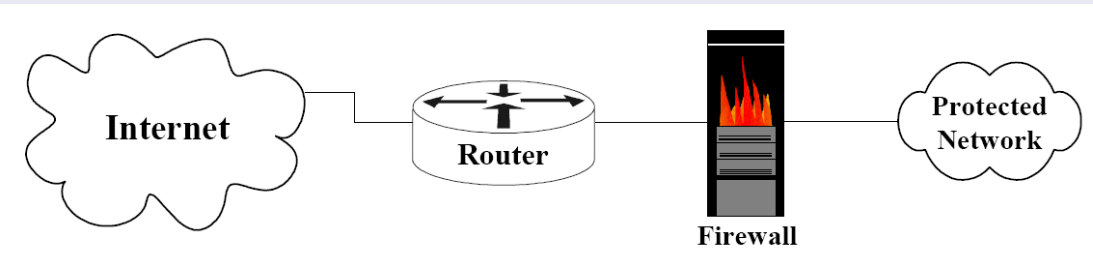
Backbone



Frontera

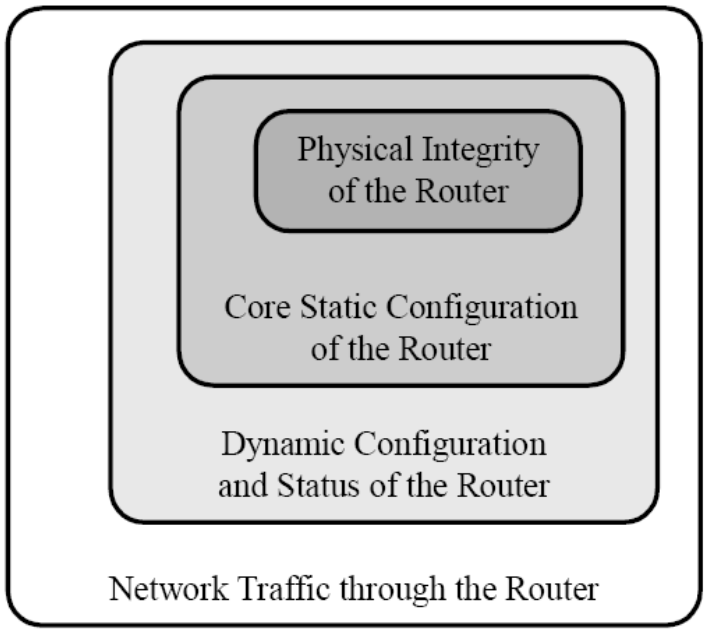


Frontera con Firewall



Capas de seguridad

Router Security Layers



Corresponding Access

- Physical access
- Electrical access

- Administrative access
- Software updates

- Routing protocols

- Access to the network that the router serves.

Seguridad física

- Designar la personal para actividades de instalación, desinstalación.
- Designar la persona para realizar actividades de mantenimento.
- Designar la persona para realizar la conexión f'isica.
- Definir controles de colocación y usos de la consola y los puertos de acceso.
- Definir procedimientos de recuperación ante eventualidades físicas.

Seguridad de configuración estática

- Designar la(s) persona(s) que accede(n) al router vía consola o en forma remota.
- Designar la persona con privilegios de administración.
- Definir procedimientos para realizar cambios a la configuración.
- Definir políticas de password de usuario y administrador.
- Definir protocolos, procedimientos y redes para acceso remoto.
- Definir plan de recuperación que incluya responsabilidades individuales ante incidentes.
- Definir políticas de revisión de bitácoras.
- Definir procedimientos y limitaciones del monitoreo remoto (SNMP).

Seguridad de configuración estática

- Definir directrices para la detección de ataques directos.
- Definir políticas de administración e intercambio de información (Protocolos de ruteo, RADIUS, SNMP, TACAS+, NTP).
- Definir políticas de intercambio de llaves de encriptación.

Seguridad de configuración dinámica

- Identificar los servicios de configuración dinámica del router, y las redes permitidas para accesar dichos servicios
- Identificar los protocolos de routeo a utilizar, y sus esquemas de seguridad que proveen.

Seguridad de configuración dinámica

- Designar mecanismos y políticas de actualización del reloj (manual o por NTP).
- Identificar los algoritmos criptográficos autorizados para levantar VPN's.

Seguridad en servicios de red

- Enumerar protocolos, puertos y servicios a ser permitidos o filtrados en cada interface, así como los procedimientos para su autorización.
- Describir procedimientos de seguridad y roles para interactuar con proveedores externos.

Respuesta a incidentes

- Enumerar a las personas u organizaciones ser notificadas en caso de una red comprometida.
- Identificar la información relevante a ser capturada y retenida.
- Definir procedimientos de respuesta, autoridades y los objetivos de la respuesta después de un ataque exitoso, incluir esquemas de preservación de la evidencia (cadena de custodia).

Seguridad en servicios de red

- Enumerar protocolos, puertos y servicios a ser permitidos o filtrados en cada interface, así como los procedimientos para su autorización.
- Describir procedimientos de seguridad y roles para interactuar con proveedores externos.

loopback

- Enumerar a las personas u organizaciones ser notificadas en caso de una red comprometida.
- Identificar la información relevante a ser capturada y retenida.
- Definir procedimientos de respuesta, autoridades y los objetivos de la respuesta después de un ataque exitoso, incluir esquemas de preservación de la evidencia (cadena de custodia).

Seguridad en servicios de red

- Enumerar protocolos, puertos y servicios a ser permitidos o filtrados en cada interface, así como los procedimientos para su autorización.
- Describir procedimientos de seguridad y roles para interactuar con proveedores externos.

Control de acceso a usuarios

- Authentication (Autenticación)
- Authorization (Autorización)
- Accounting (Contabilidad)

Servidores para AAA

- RADIUS
- TACAS+
- Kerberos

Example

South(config)# enable secret rl3r6Ed
South(config)# username bethadmin password hs0o3TaG
South(config)# username johnadmin password an0!h3r(
South(config)# banner motd ∧T
.
.
∧T
South(config)# tacacs-server host 14.2.6.18
South(config)# tacacs-server key lr3@1yh8nw9@swD
South(config)# aaa new-model
South(config)# aaa authentication login default tacacs+ local
South(config)# aaa accounting exec default start-stop tacacs+
South(config)# aaa accounting exec remoteacc wait-start tacacs+
South(config)# aaa accounting connection default start-stop tacacs+
South(config)# aaa accounting system default start-stop tacacs+
South(config)# aaa accounting commands 15 default stop-only tacacs+

Example

South(config)# access-list 91 permit 14.2.9.0 0.0.0.255 log
South(config)# access-list 91 permit 14.2.10.0 0.0.0.255 log
South(config)# access-list 91 deny any log
South(config)# line con 0
South(config-line)# transport input none
South(config-line)# exec-timeout 5 0
South(config-line)# login local
South(config-line)# exit
South(config)# line vty 0 4
South(config-line)# access-class 91
South(config-line)# exec-timeout 5 0
South(config-line)# login local
South(config-line)# transport input telnet
South(config-line)# login authentication remotelist
South(config-line)# accounting exec remoteacc
South(config-line)# exit

Example

South(config)# line aux 0
South(config-line)# transport input none
South(config-line)# login local
South(config-line)# exec-timeout 0 1
South(config-line)# no exec
South(config-line)# end

Example

Central(config)# enable secret 3rRsd$y
Central(config)# username fredadmin password d$oyTld1
Central(config)# username bethadmin password hs0o3TaG
Central(config)# username johnadmin password an0!h3r(
Central(config)# service password-encryption
Central(config)# banner motd ∧T
Legal Notice: Access to this device is restricted. .
.
∧T
Central(config)# radius-server host 14.2.6.18
Central(config)# radius-server key i*Ma5in@u9ps5wD
Central(config)# aaa new-model
Central(config)# aaa authentication login default radius local
Central(config)# aaa accounting exec default start-stop radius
Central(config)# aaa accounting exec remoteacc wait-start radius

Example

Central(config)# aaa accounting connection default start-stop radius
Central(config)# access-list 91 permit 14.2.9.0 0.0.0.255 log
Central(config)# access-list 91 deny any log
Central(config)# line con 0
Central(config-line)# transport input none
Central(config-line)# exec-timeout 5 0
Central(config-line)# login local
Central(config)# line vty 0 4
Central(config-line)# access-class 91
Central(config-line)# exec-timeout 5 0
Central(config-line)# login local
Central(config-line)# transport input telnet
Central(config-line)# accounting exec remoteacc
Central(config)# line aux 0

Example

Central(config-line)# transport input none
Central(config-line)# login local
Central(config-line)# exec-timeout 0 1
Central(config-line)# no exec
Central(config-line)# end