Firewalls

Redes 2

Firewalls

- Ya sea que se trate de un dispositivo dedicado que actúe como firewall, o bien se un dispositivo con funcionalidades de firewall y otros servicios compartidos, el propósito principal de un firewall es:

1. Detener el ingreso a un área de la red al tráfico considerado como peligroso. Dicha área puede ser tan grande como todo la red de una empresa, o tan pequeña como una simple subred de la red interna.
2. Permitir el flujo de tráfico deseado, normalmente dejando monitoreado dicho tráfico.

Firewalls

- Los firewalls forman parte de una estrategia de seguridad llamada “defense in Depth”, donde el firewall es parte de una línea de defensa contra atacantes.
- Tomar en cuenta que un solo punto de defensa en la red no es deseado porque implica un único punto de fallo.
- Una buena práctica es mantener las políticas de seguridad por escrito antes de implementarlas en un firewall, obedeciendo las necesidades de la organización.

Security policies

- Una buena estrategia de seguridad no debe de ser estática, y las políticas de seguridad en el firewall tampoco deberían serlo.

- Es responsabilidad del administrador de red mantenerse informado de las últimas amenazas de red, y asegurar que los firewalls están preparados para tratarlas.

- Hablemos de los pros y contras de los firewalls…

Pros:

- Detienen a usuarios no autorizados de ingresar a la red.
- Detienen virus, malware, trojan horses, y similiares en la entrada de la red.
- Es mucho más fácil para el hardware y para los humanos detener este tipo de ataques en el perímetro de la red en lugar de combatirlos una vez ya estén dentro de la red.
- Previene que usuarios no autorizados para ingresar a la red tengan acceso a datos sensibles sobre los cuáles no tienen permisos.
- Previene que atacantes potenciales ganen acceso a información como el esquema de direccionamiento de la red interna, por medio de ataques de descubrimiento (recon attacks).

Contras

- Lograr una configuración adecuada (fine-tuning) desde la implementación inicial es un trabajo costoso:
  - Se debe permitir y garantizar que los datos legítimos fluyan a través del firewall.
  - Se debe permitir y garantizar que todos los usuarios legítimos accedan a los datos que tienen permiso de acceder, mientras se previene el acceso a información no autorizada.
  - Se debe garantizar que los servicios de red y aplicaciones funcionen como lo hacían antes de implementar el firewall.

Stateless Packet Filtering

- Stateless filtering es conocido también como:
    - Static packet filtering
    - Static filtering
    - Packet filtering

Access list!

- Cuando se utilizan ACL, se pone en acción el stateless filtering.

- Nuestra experiencia en ACL nos dice que es común filtrar paquetes basado en cualquiera de los siguientes datos:

  - Source IP address
  - Destination IP address
  - Source port number
  - Destination port number
  - Protocol number

Stateless filtering

- Es fácil de implementar
- No se necesita hardware especializado o alguna imagen de IOS especializada.
- ¿Por qué existe entonces un “stateful filtering”?

¿Por qué Stateful filtering?

- Una conexión iniciada por un host interno es mucho más probable que sea una conversación legítima que otra originada por un host externo a la red.
- Por lo tanto nos interesa conocer si un paquete entrante es parte de una conversación ya existente o el paquete entrante esta tratando de iniciar una conversación.
- ACLs son buenas permitiendo o denegando paquetes en base a puertos estáticos, pero no son buenas tratando puertos dinámicos utilizados por algunas aplicaciones (por ejemplo FTP).
- Stateless filtering es vulnerable a ataques de IP spoofing, ya que no existe memoria o listado de IPs previamente conectadas.

Stateful packet filtering

- Monitorea los estados de conexión TCP, incluyendo los números de secuencia TCP, lo cuál es vital para prevenir ataques basados en TCP.
- Básicamente, los stateful firewalls permiten que los hosts internos inicien una conversación con hosts externos, pero no permite que hosts externos inicien conversaciones con hosts internos.
- Lo anterior se logra a través de una “session table”, conocida como “state table”. Cuando una conversación entra a un estado de inactividad, esta es eliminada.

State table

Está conformada por:

- Source and destination IP addresses
- Source and destination port numbers
- El estado de la conexión

State table

Source IP	Source Port	Destination IP	Destination Port	Connection State
192.168.1.1	1001	100.1.1.1	80	Established
192.168.1.2	1030	110.1.1.1	80	Established
192.168.1.3	1000	120.1.1.1	80	Established

Stateful packet filtering

- No permite ingresar a la red paquetes externos SYN.
- Únicamente permite el ingreso de paquetes con el flag ACK configurado si la tabla de estado indica que un host interno inició el TCP handshake.
- Adicionalmente, paquetes TCP con números de secuencia fuera de un rango esperado serán descartados (dropped).

Stateful filtering

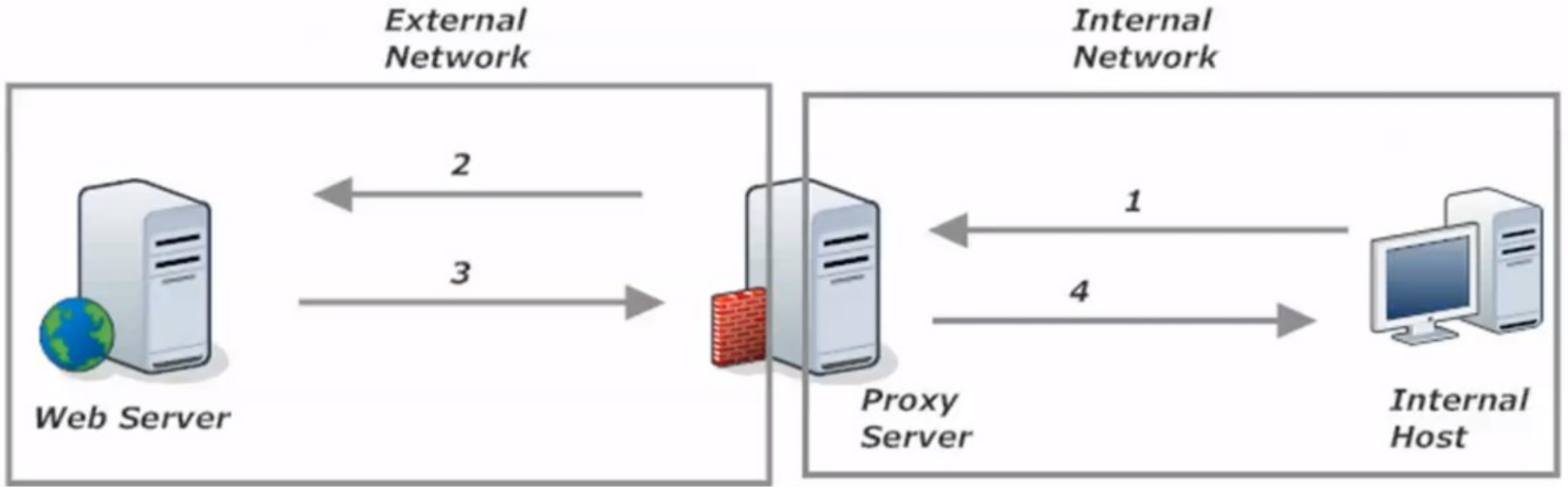
- Beneficia la utilización de aplicaciones y protocolos L7 que utilizan puertos dinámicos, como FTP.
- FTP utiliza puertos TCP 20 y 21, y dependiendo si está configurado de forma pasiva o activa, utiliza puertos aleatorios.
- Un firewall con stateful filtering reconocerá la construcción del canal FTP y permitirá que se complete la transferencia de información.

Proxy firewalls

- Cuándo votas por medio de un proxy, otra persona está votando en tú lugar.
- Cuándo un Proxy Firewall es implementado, dicho dispositivo se conectara al destino externo (outside) en lugar del host origen (o quizás no permitirá conectarse…).

Proxy firewalls

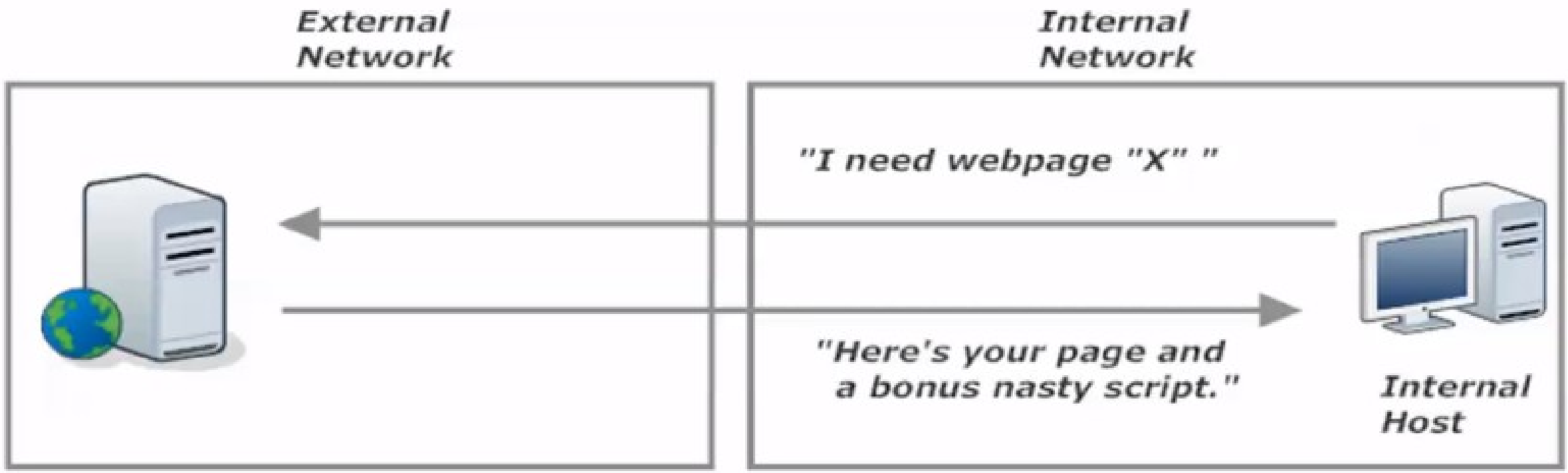
- El proxy firewall es “the middleman” entre nuestra red interna de usuarios y los destinos fuera de la red.
- Este “middleman” realiza pasos adicionales en la conexión, pero es en nombre de la seguridad!

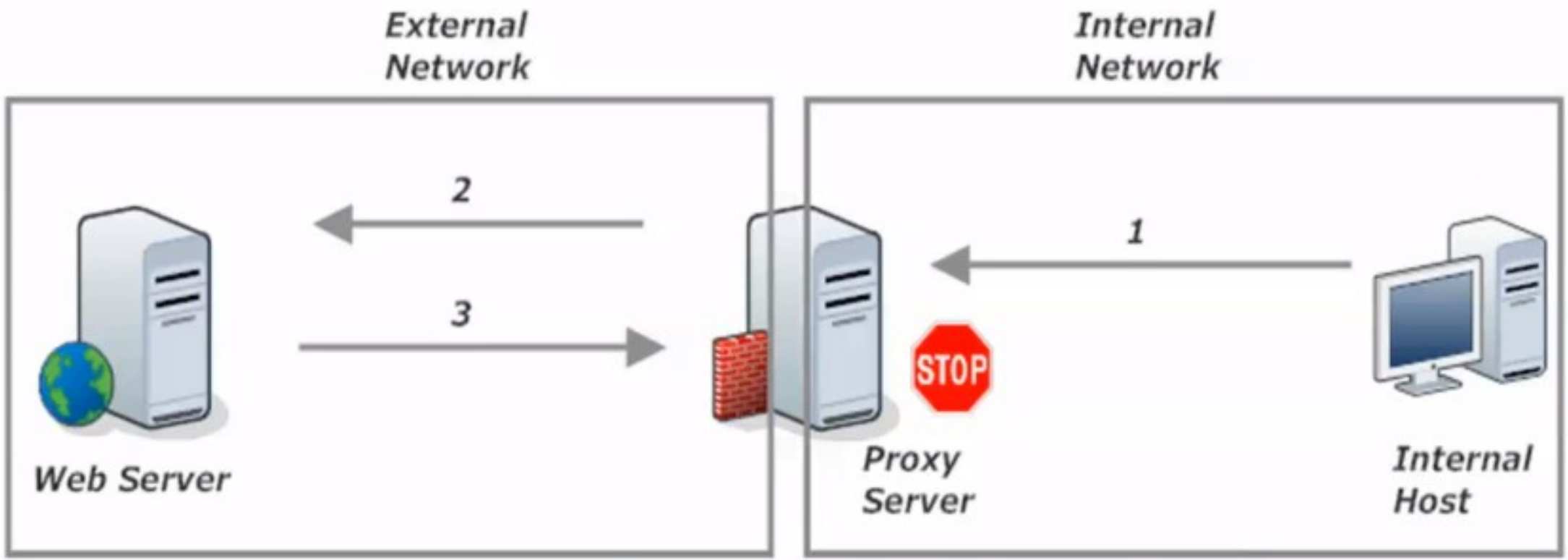


Beneficios de los proxy firewall

- Defensa poderosa contra website-based attacks, particularmente ataques de cross-site scripting (XSS). En estos ataques un script malicioso es inyectado en las páginas web.

- Cuando un visitante “desprotegido” visita el sitio, el script es activado, y ocasiona graves riesgos de seguridad dependiendo la sensibilidad de los datos que se alimentan desde el sitio web vulnerado.


External Network
Internal Network
"I need webpage "X" "
"Here's your page and a bonus nasty script."
Internal Host

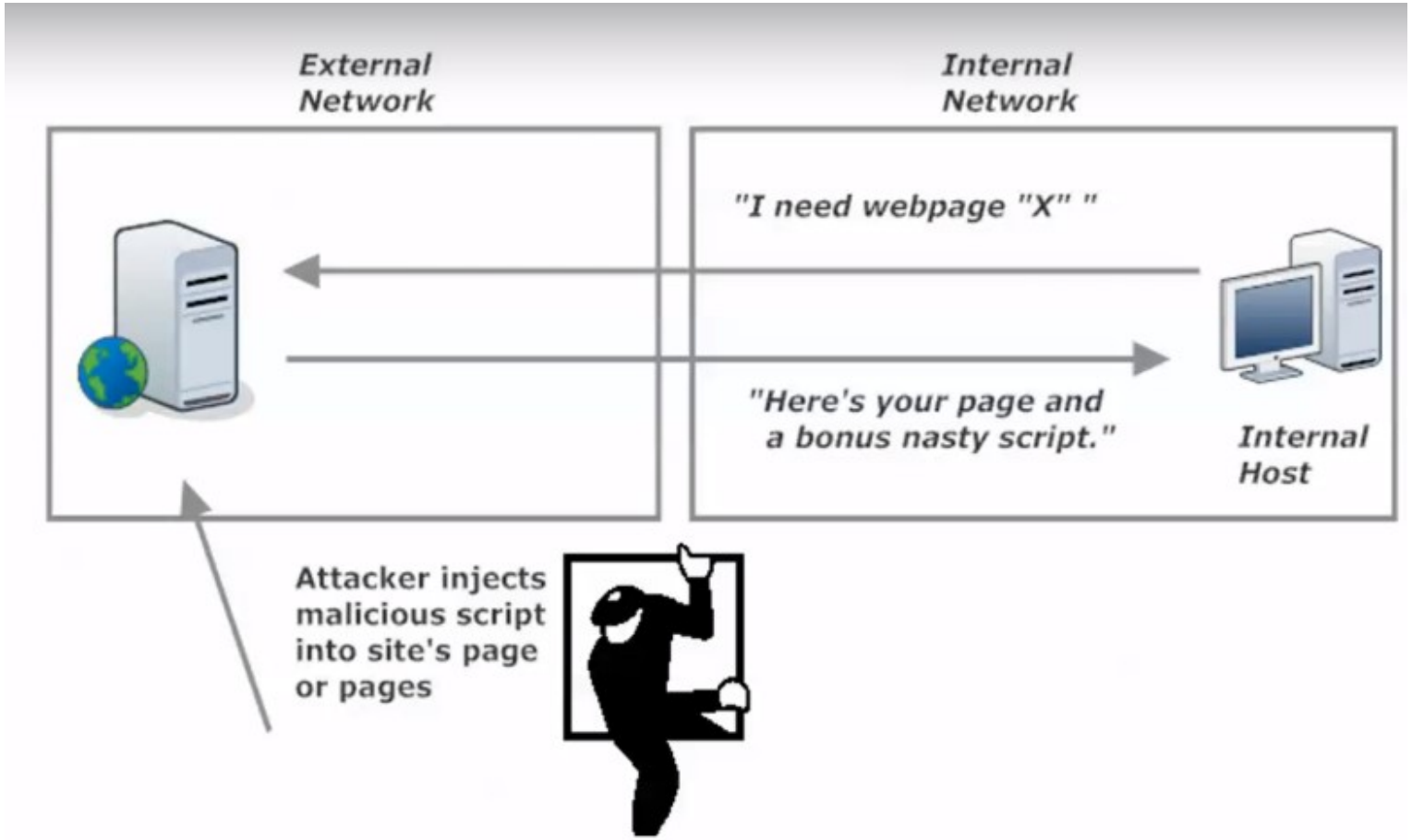


4: "This webpage is dirty. I'll block it and notify the network admins."

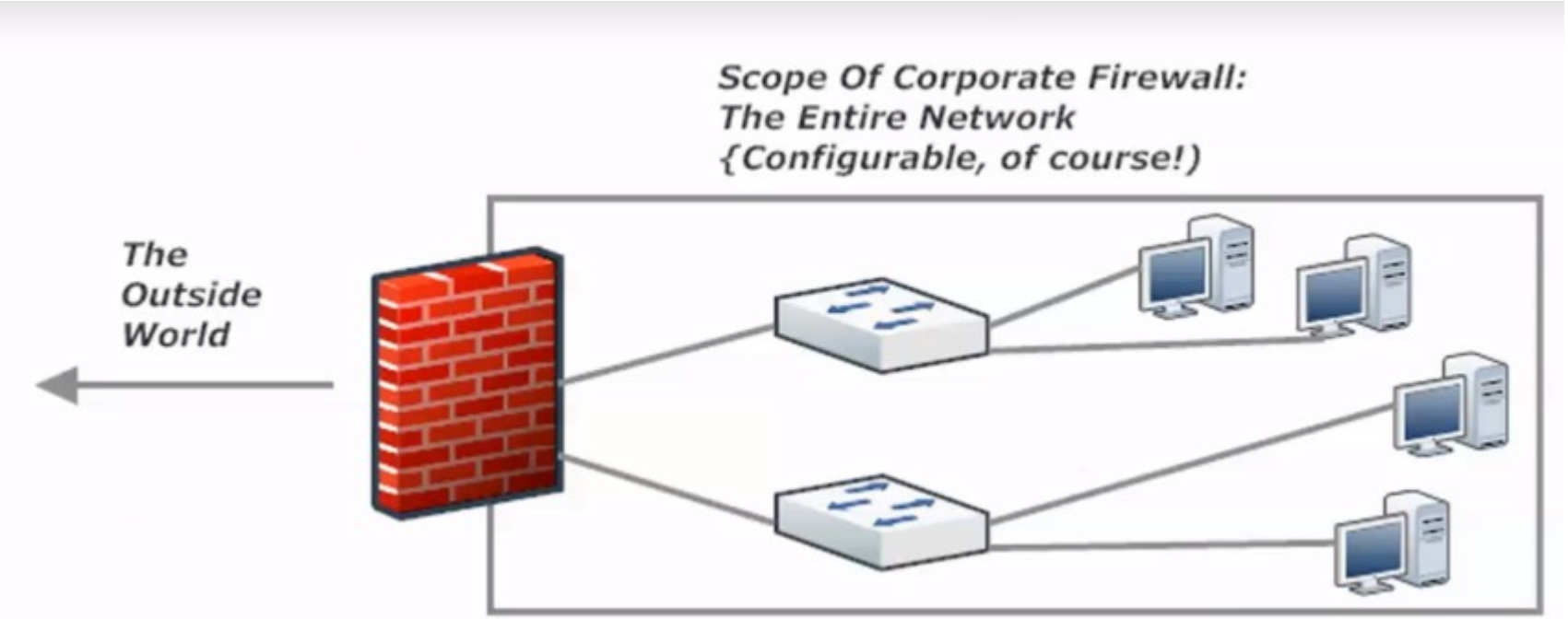
XSS attacks

- Existen dos víctimas:
  - El website que aloja el script
  - El visitante del sitio infectado
- El script pudo llegar al sitio desde la red interna o desde la red externa explotando alguna vulnerabilidad.

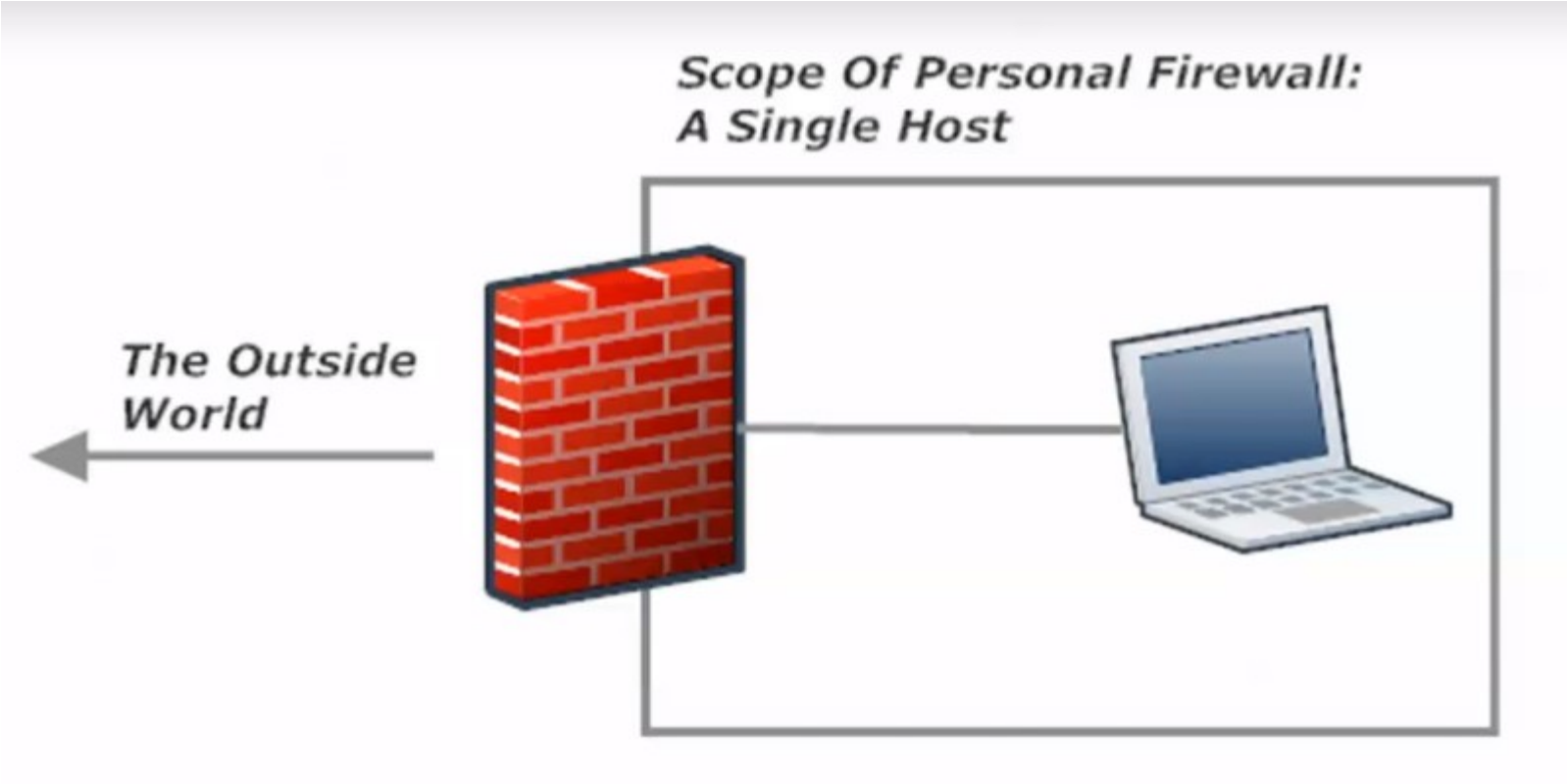
XSS attacks


External Network
Internal Network
"I need webpage "X" "
"Here's your page and a bonus nasty script."
Internal Host
Attacker injects malicious script into site's page or pages

Scope del Firewall Corporativo



Scope del Firewall Personal



Pros de los Firewall Personales

- Las políticas de seguridad pueden ser definidas en base a las necesidades individuales del usuario.
- Extender la protección de un firewall a ubicaciones de red donde no existen premisas de seguridad (redes sin protección de un Firewall perimetral!). Por ejemplo: redes wifi abiertas como Aeropuertos, Hoteles, Cafeterías, etc.
- Permite configurar reglas personales para que sitios no conocidos o redes no conocidas tengan acceso al computador personal.
- Permite configuración de whitelists y blacklists de aplicaciones y sitios.

Contras del firewall personal

- Software maliciosos pueden vulnerar y configurar reglas en el firewall personal. Sobre todo si ya existía el software malicioso previo a instalar el firewall.
- Necesita también de configuración precisa (fine-tuning) para lograr un nivel de seguridad alta.

Recomendación/Buena práctica:

- Implementar firewalls personales con políticas asociadas a las políticas de seguridad del firewall corporativo.

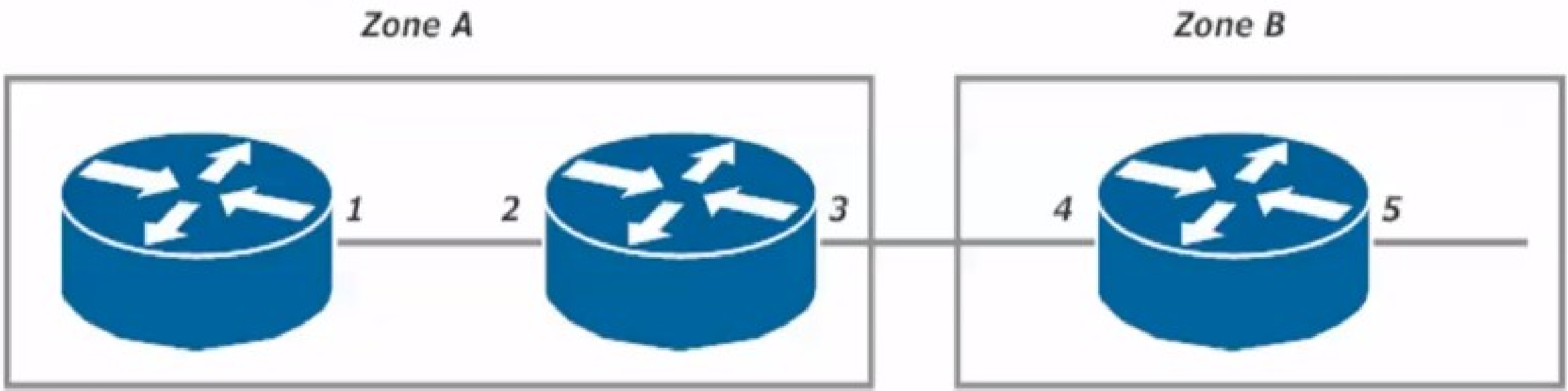
Introducción a Cisco IOS Zone-Based Firewall

¿Qué es una zona?

- Es un grupo lógico de interfaces
- Una zona no necesariamente contiene cada interfaz de un router
- Una interfaz puede pertenecer únicamente a una zona

Dos defaults importantes:

- El tráfico fluye libremente entre interfaces en la misma zona.
- El tráfico no fluye entre interfaces en diferentes zonas.



Interfaces 1, 2, and 3 can exchange traffic as can interfaces 4 and 5. By default, traffic could not flow between interfaces 3 and 4.

¿Qué pasa con el tráfico generado en el router local?

- A esto se le llama “self zone”

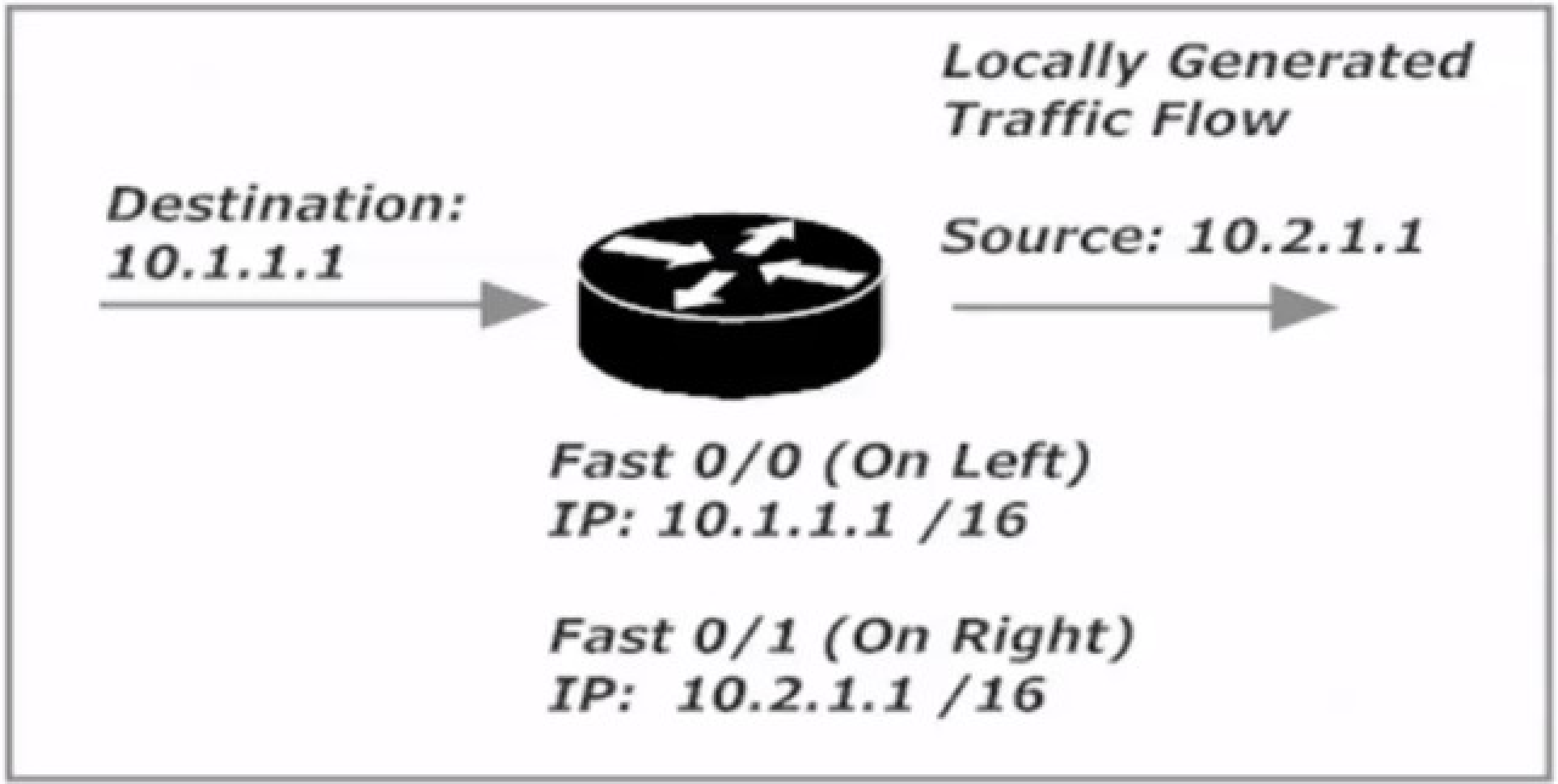
- Esta zona engloba el tráfico destinado de una dirección IP presente en el router local (“entrando a la self zone”) y el tráfico generado por el router (“saliendo de la self zone”). Todo este tráfico se permite por defecto, porque es el tráfico generado localmente en el router.

Ejemplos de self zone

1. Controlar el tráfico que fluye hacia el router (tráfico de administración, como conexiones SSH, Telnet, SNMP, etc.).

2. Tráfico desde el router hacia otras zonas (como actualizaciones de software o pings hacia otras zonas).

The Self Zone

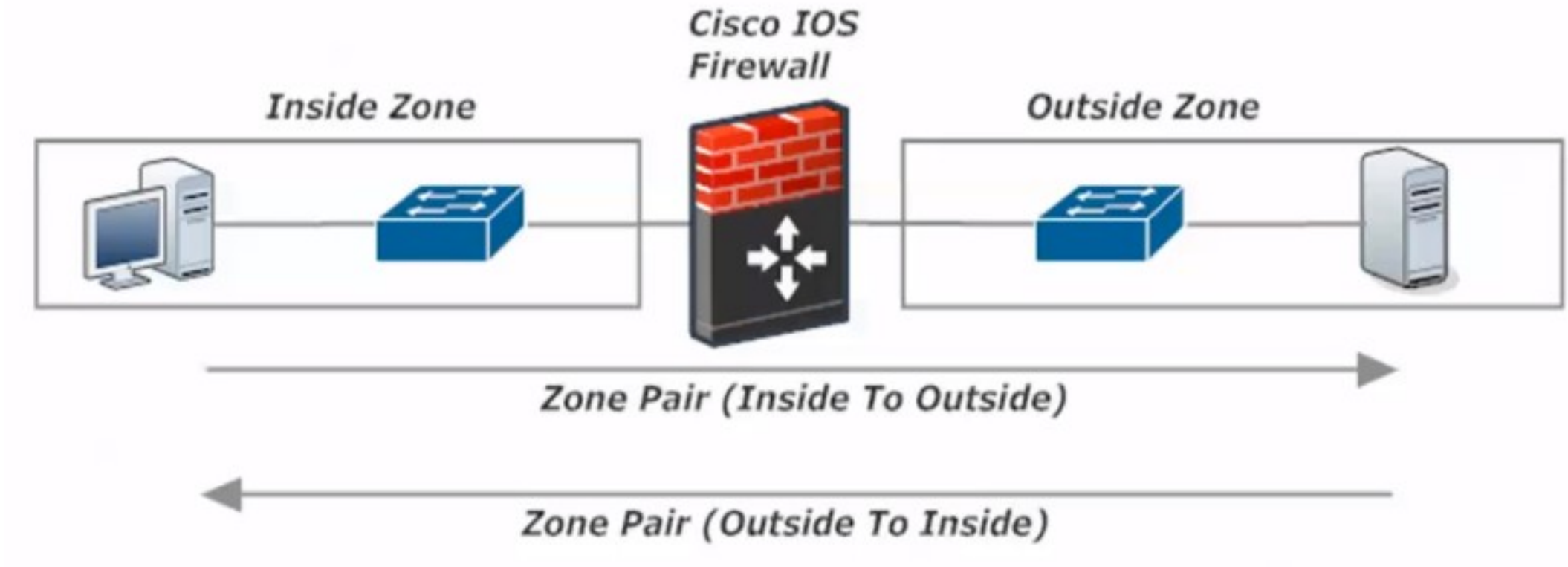


The Zone Pairs

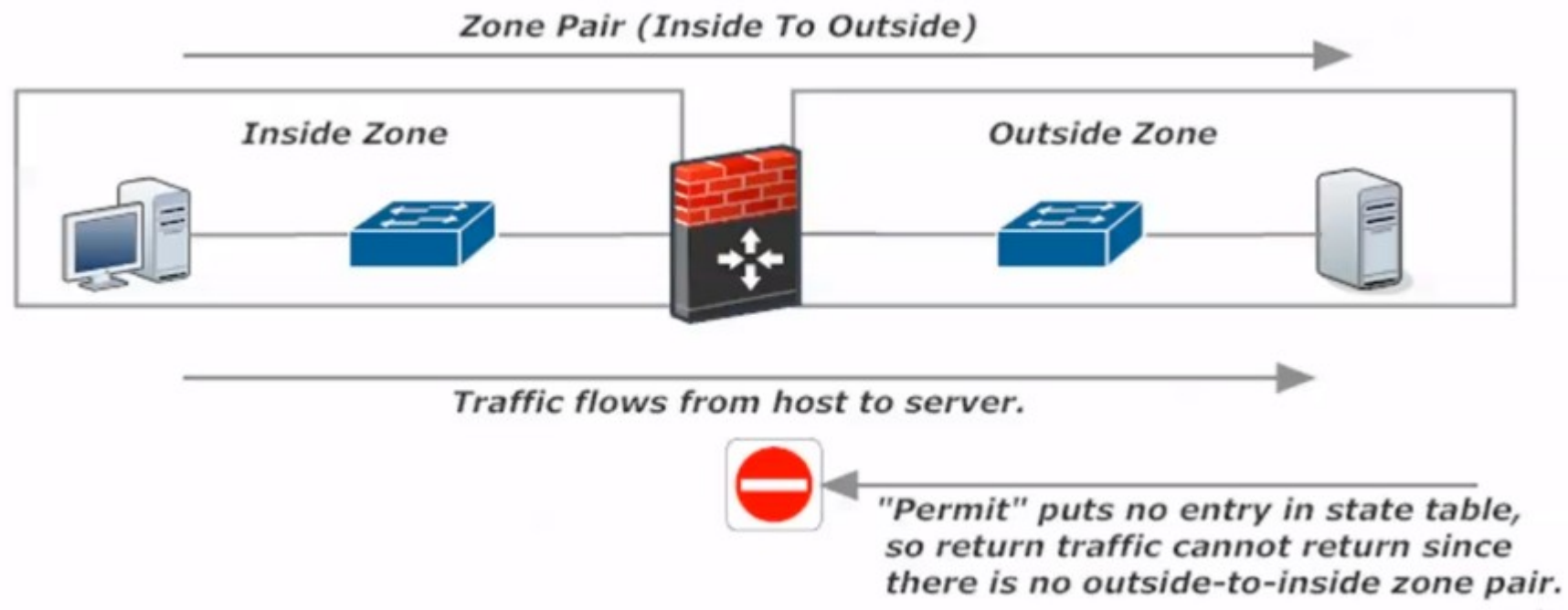
- El tráfico inter-zona (entre zonas) no es permitido por defecto.
- Pero es muy extraño que existan redes que no permitan comunicarse entre diferentes zonas….
- Está comunicación únicamente se logra a través de una “zone pair” (paridad de zonas), que es una configuración unidireccional de reglas que es aplicada al tráfico que viaja “entre zonas”.
- Una zone pair solo apunta a una dirección, por lo tanto, si necesitamos que un host inicie una transmisión hacia un servidor, y luego el servidor transmita hacia el host, necesitaremos 2 zone pairs.

Acciones entre zonas

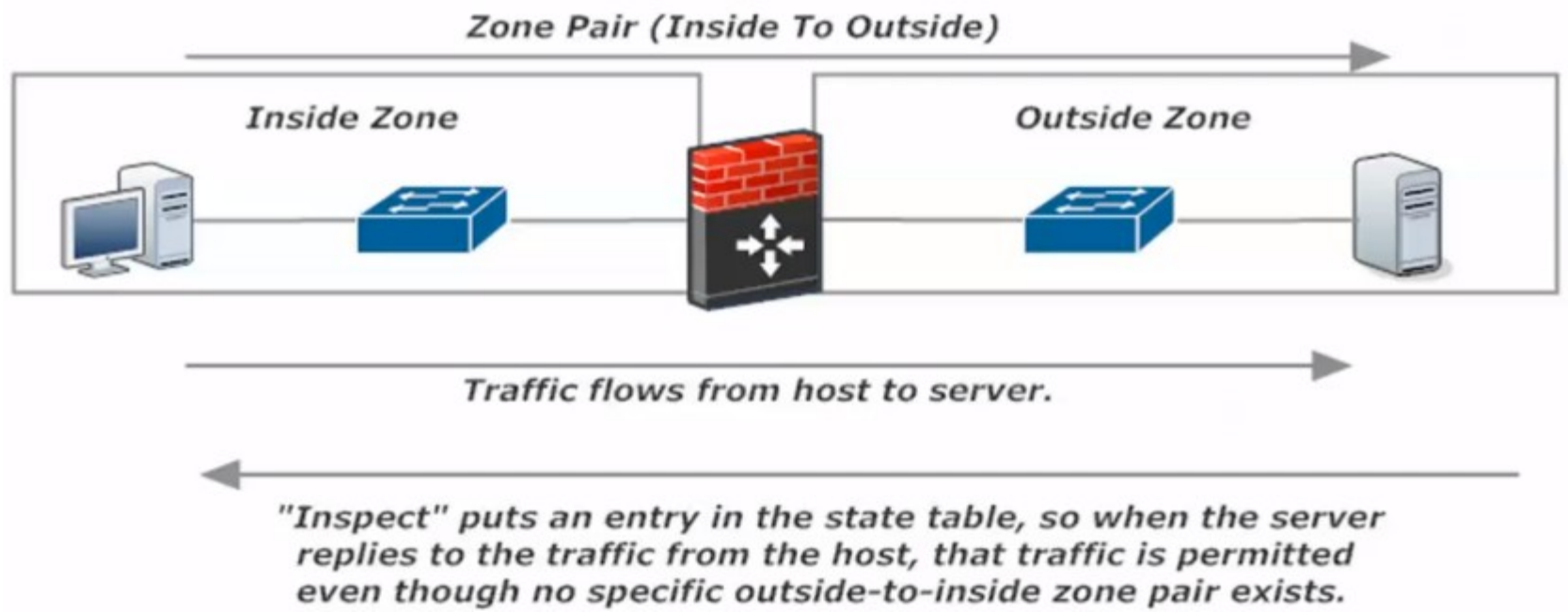
- Inspect
  - Una entrada se agrega a la stateful database únicamente para los protocolos aplicados en la política, permitiendo que las respuestas desde otra zona puedan ingresar.
- Drop
  - Acción por defecto si el tráfico no coincide con alguna política.
- Pass
  - El tráfico es permitido de una zona a otra pero no se lleva control de las sesiones.


Cisco IOS
Firewall
Inside Zone
Outside Zone
Zone Pair (Inside To Outside)
Zone Pair (Outside To Inside)

Permit: el host puede enviar tráfico al servidor, pero el servidor no puede responder, porque no se ha agregado una entrada a la tabla de estado.



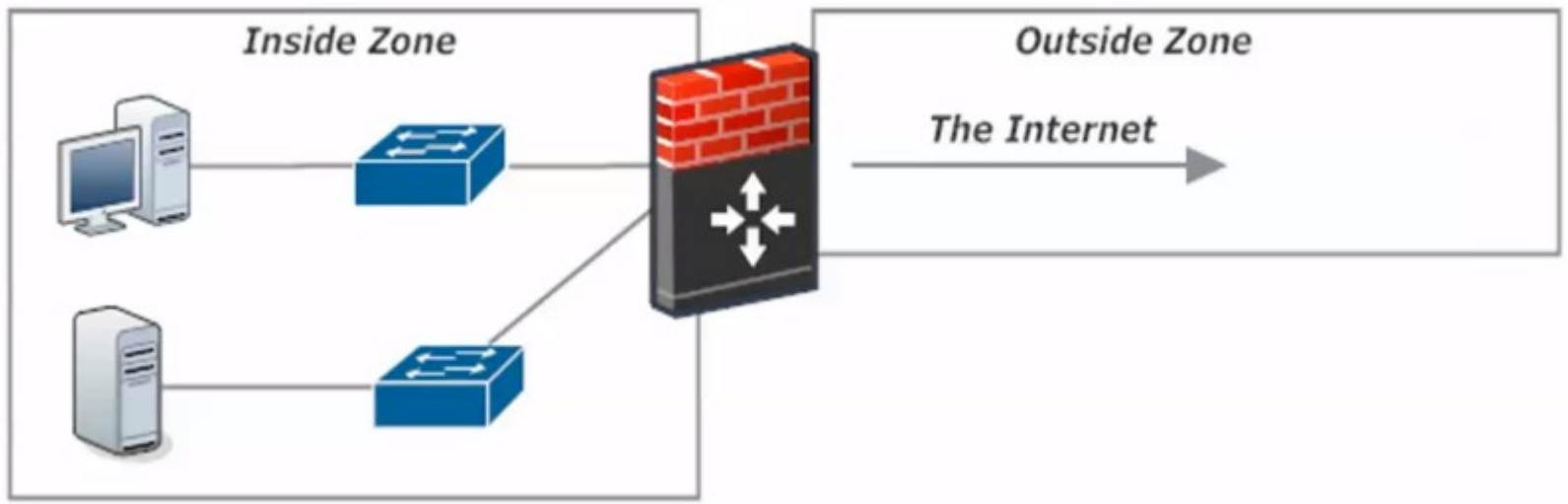
Inspect: el host puede enviar tráfico al servidor, y al realizar una entrada en la tabla de estado, el servidor puede responder al host incluso si no existe un zone pair que lo permita (outside to inside)



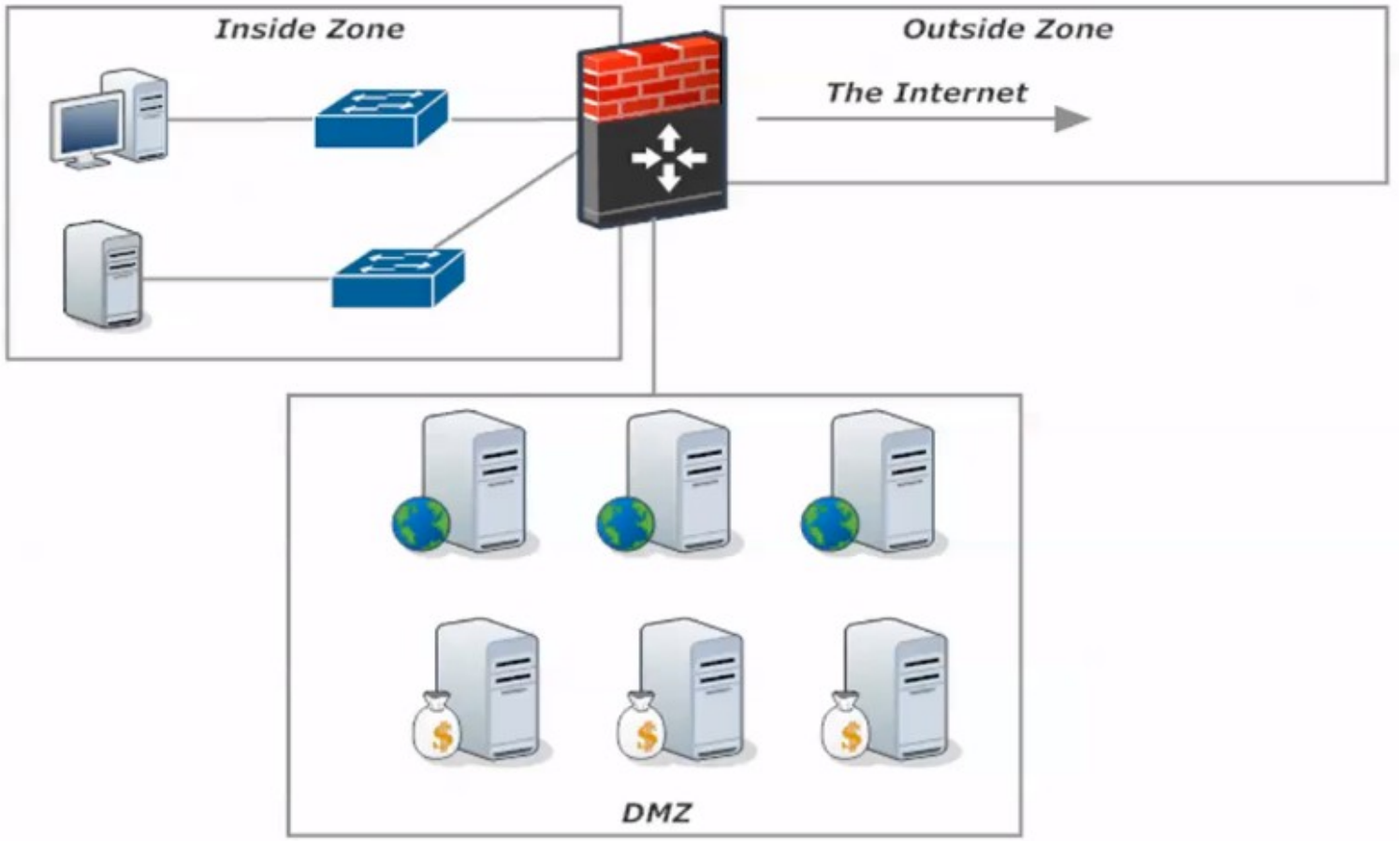
La DMZ

- La zona desmilitarizada es un segmento de nuestra red que contiene los servidores y sistemas que requieren acceso desde la outside zone.
- En lugar de conectar dichos servidores en la red interna (inside zone) y luego permitir el acceso a usuarios externos hacia dicha red interna, podemos conectarlos en la DMZ.
- Esto restringe el acceso a la zona interna mientras se permite el acceso de usuarios externos a los servidores en la DMZ.

Sin DMZ…



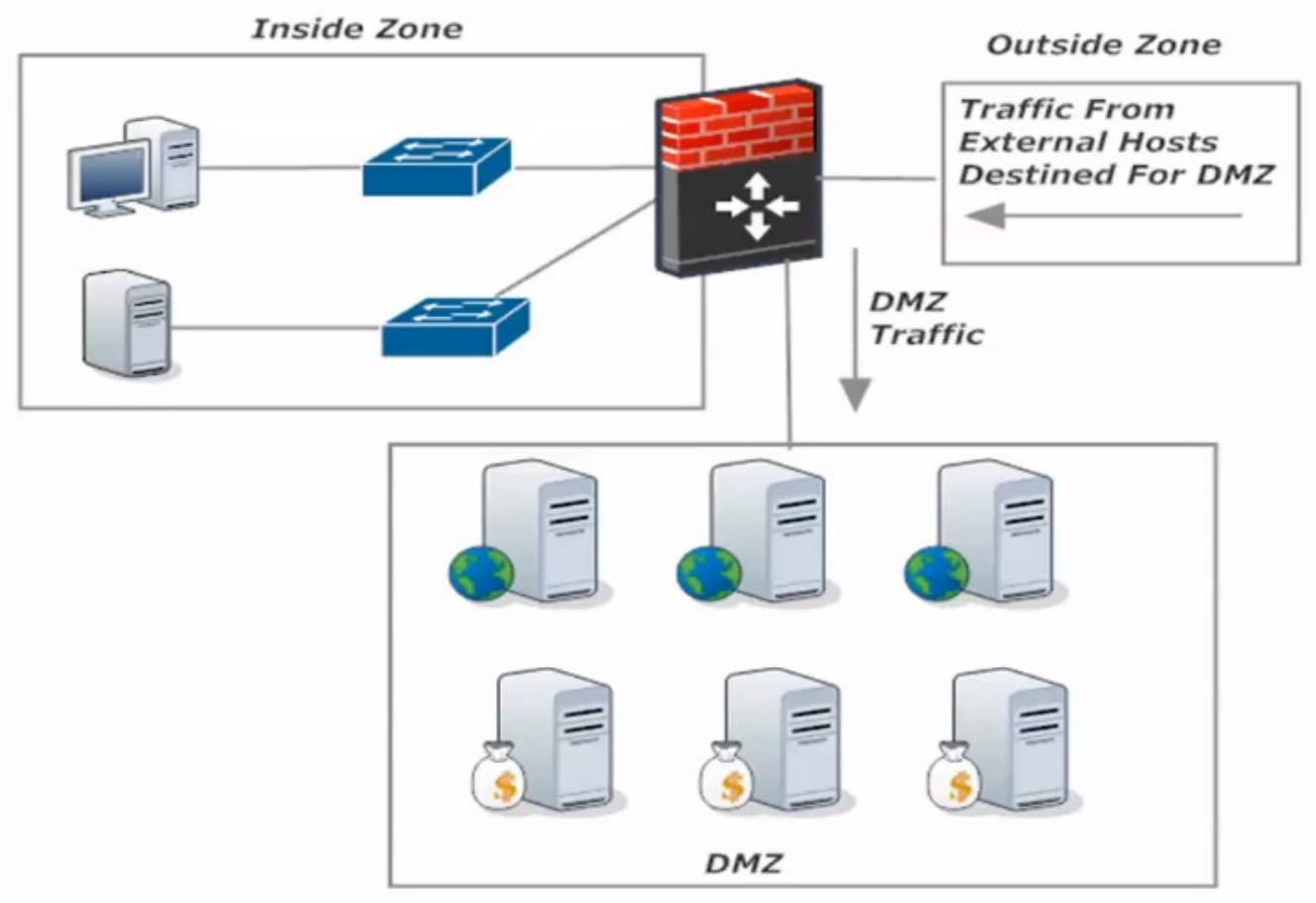
Con DMZ



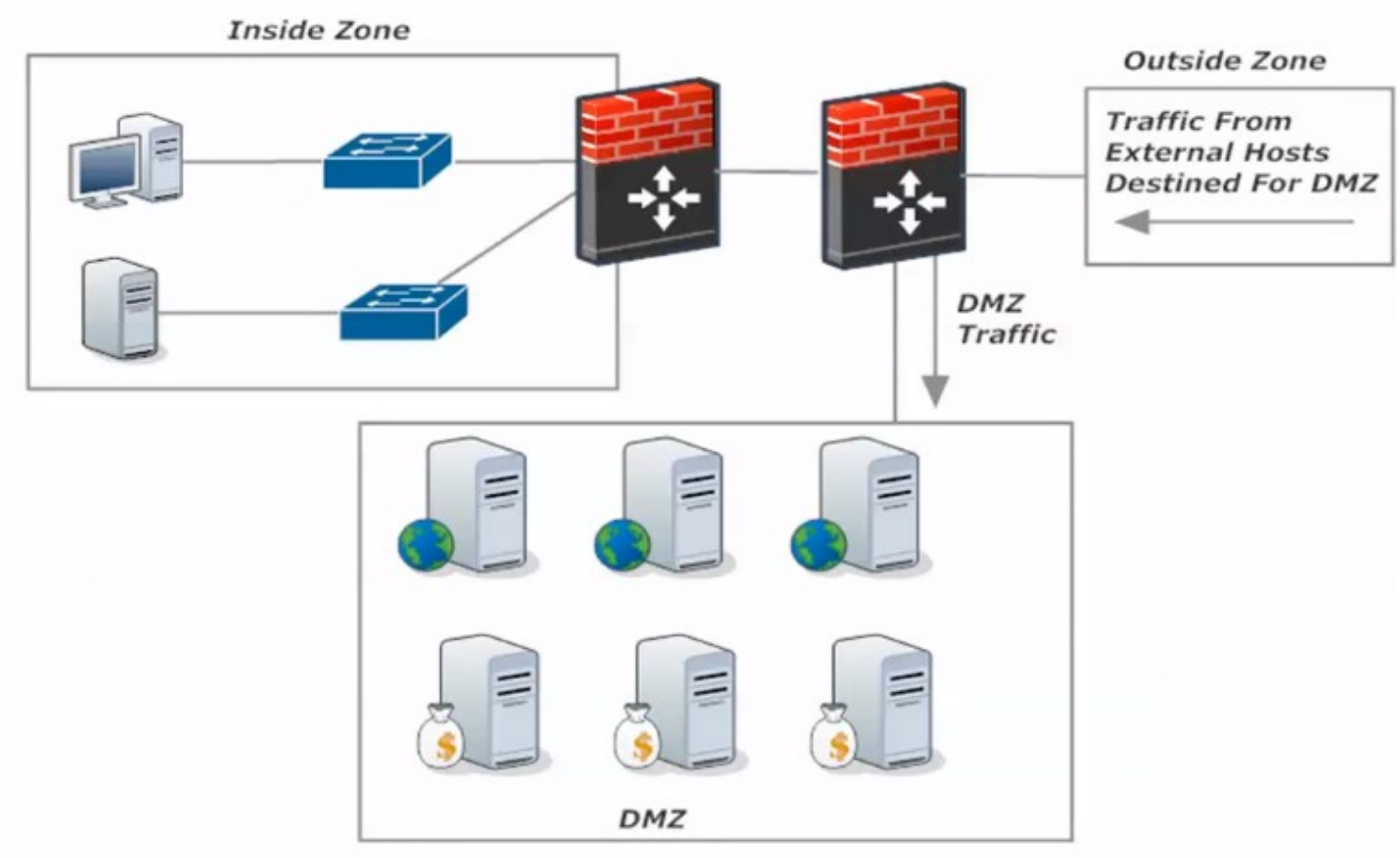
Servidor típicamente ubicados en la DMZ

- FTP servers
- Email servers
- Proxy servers
- Ecommerce servers
- DNS servers
- Web servers

Single DMZ Firewall Approach



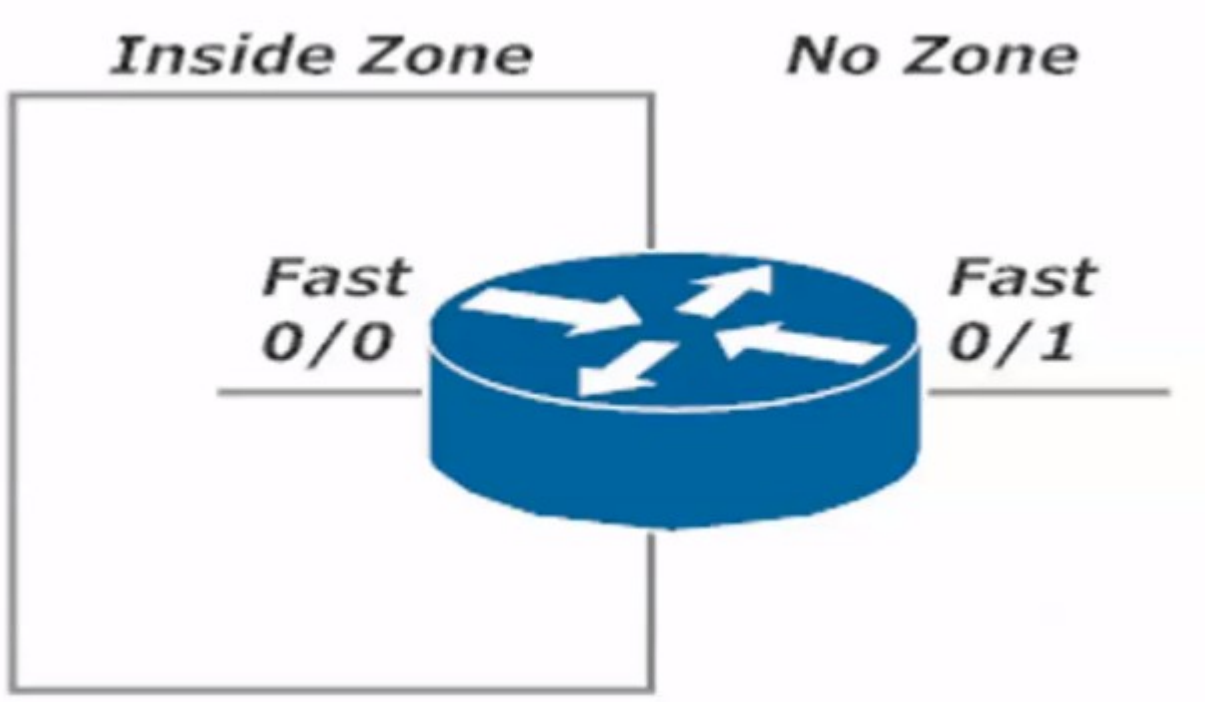
Double DMZ Firewall Approach



Notas importantes

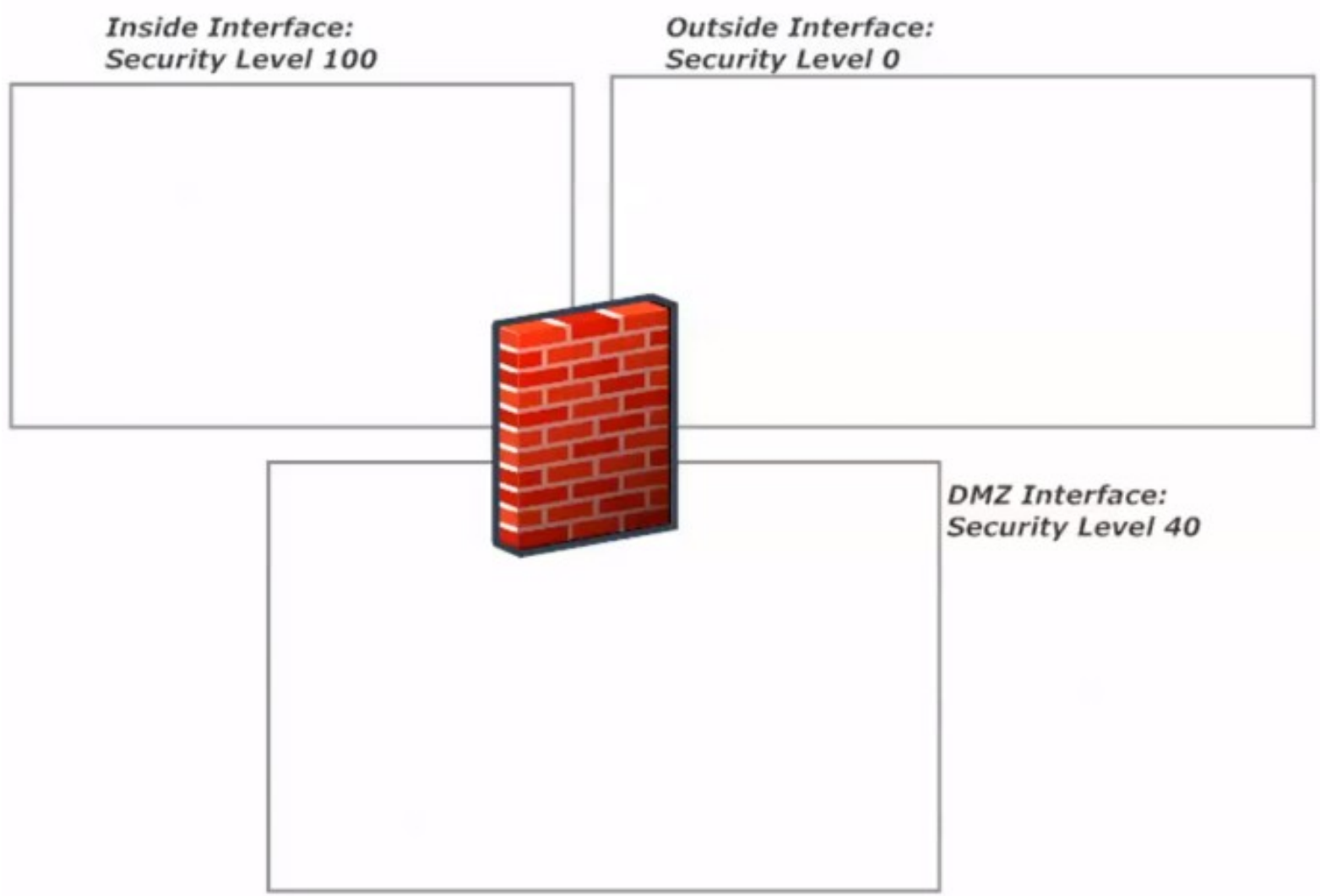
- Stateful inspection no es soportado para multicast
- Una interfaz solo puede pertenecer a una zona
- No es necesario que cada interfaz de un router corriendo ZBF tenga que pertenecer a una zona, pero pueden ocurrir problemas de conexión si no se implementa.

Problemas de no asociar zonas



The ASA

- El ASA utiliza niveles numéricos de seguridad.
- De 0 a 100, asignando 100 (comúnmente) a la interfaz conectada más confiable (most trusted) y 0 a la menos confiable (least trusted), y usualmente un número intermedio se asigna a la interfaz de DMZ.
- La interfaz outside (lest trusted) por lo general es la interfaz conectada hacia Internet.


Inside Interface:
Security Level 100
Outside Interface:
Security Level 0
DMZ Interface:
Security Level 40

Niveles numéricos de seguridad

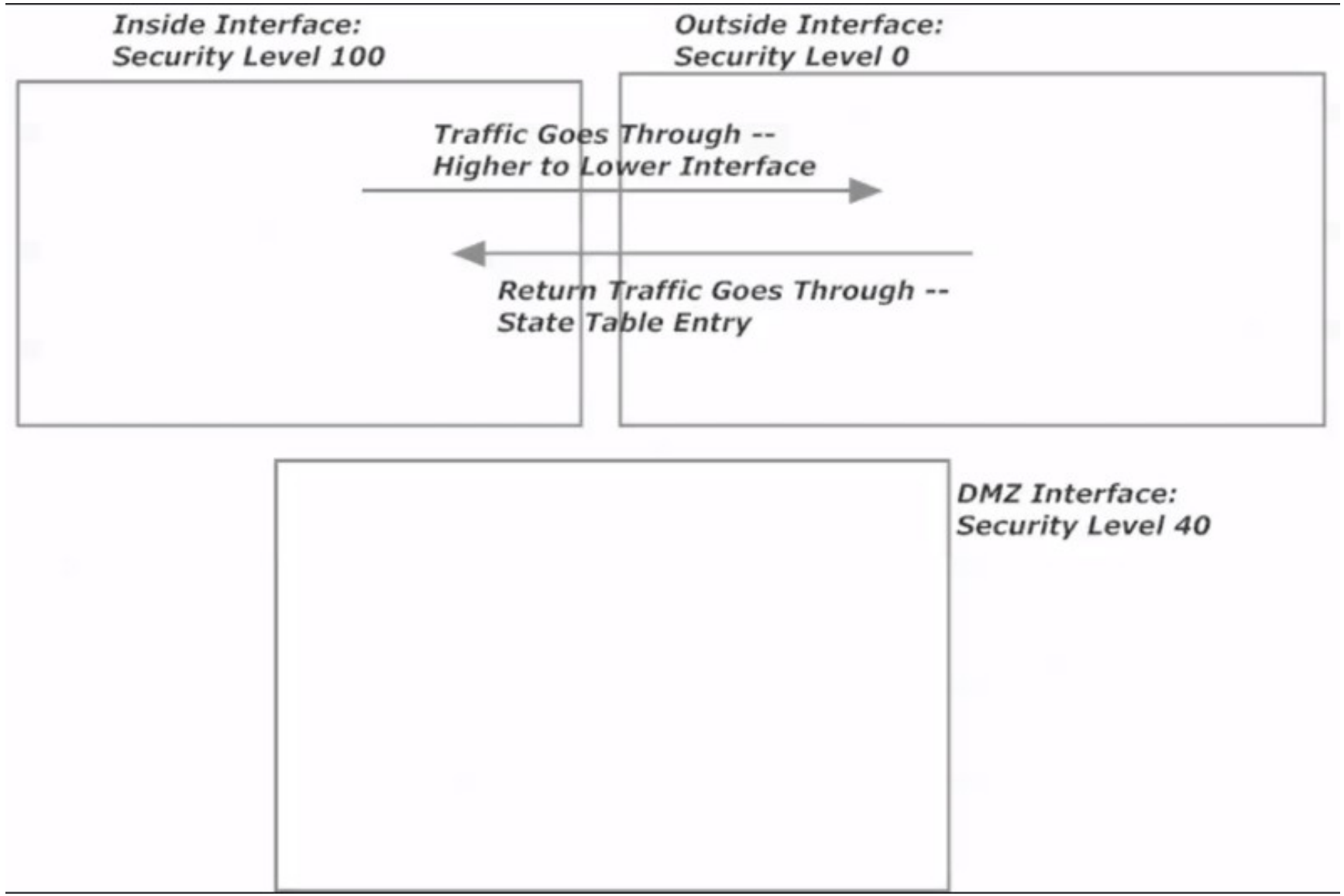
- Por defecto, el tráfico originado desde una interfaz higher-rated destinado hacia un host externo a través de una interfaz lower-rated, va a pasar.
- Los hosts internos serán capaces de iniciar comunicaciones con hosts externos, pero estos últimos no podrán responder de acuerdo a la premisa anterior.

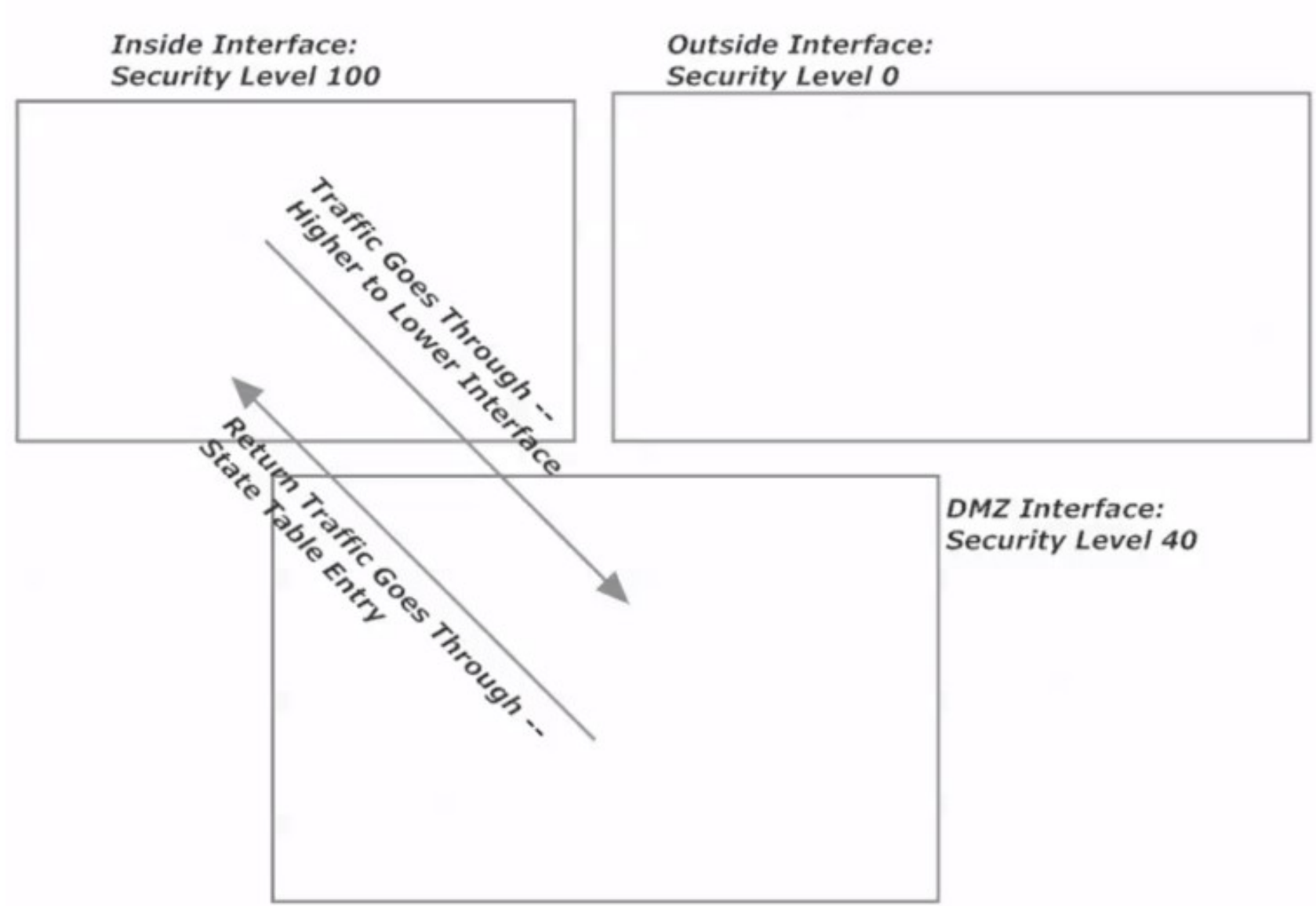
Niveles numéricos de seguridad

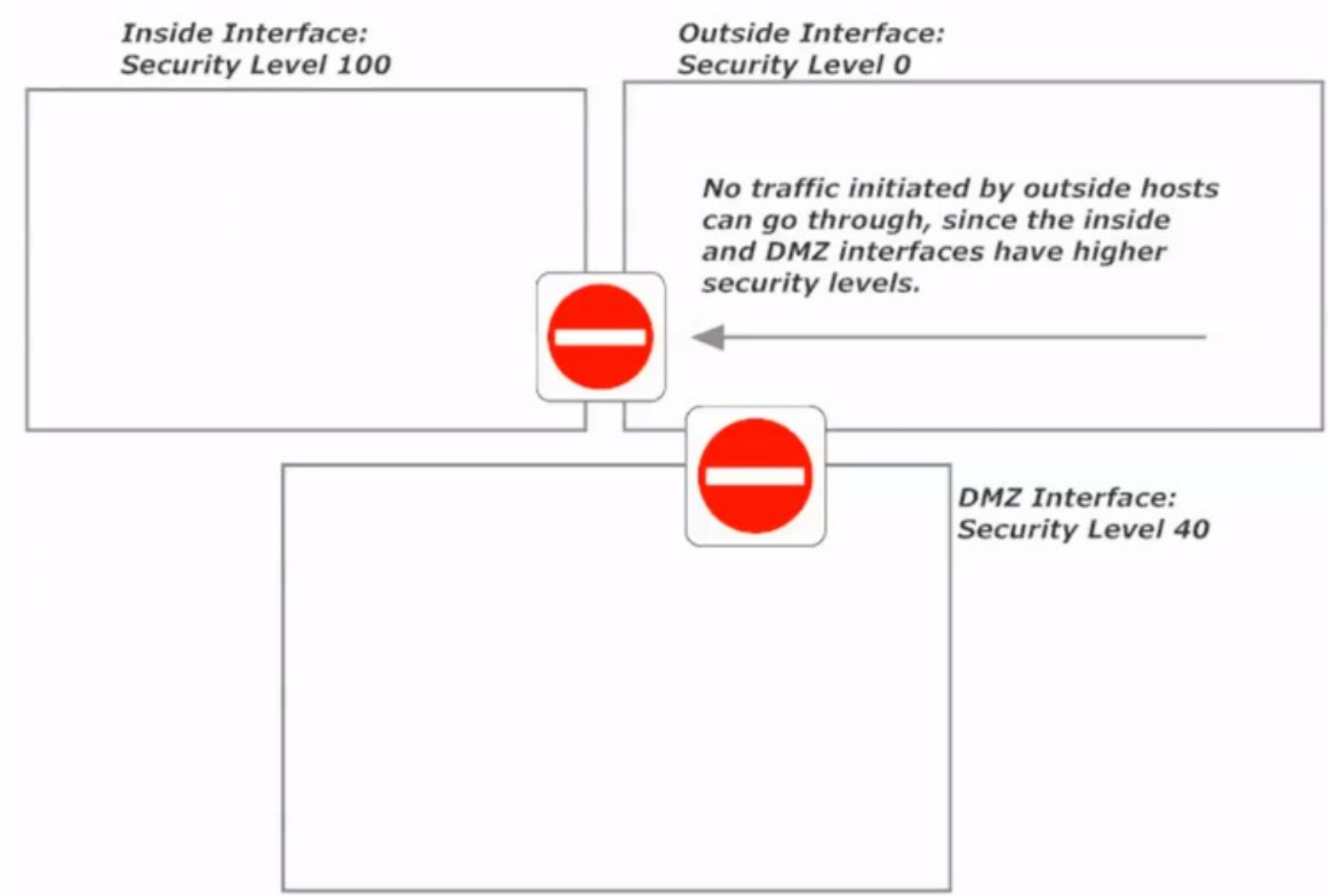
- Nota: los paquetes no pueden ser enviados desde una interfaz hacia otra interfaz si las interfaces tienen el mismo nivel de seguridad. En este caso un empate es sinónimo de perder.
- Por defecto, los hosts externos (outside) no están habilitados para iniciar comunicaciones con los hosts internos (inside) o con host de la DMZ.

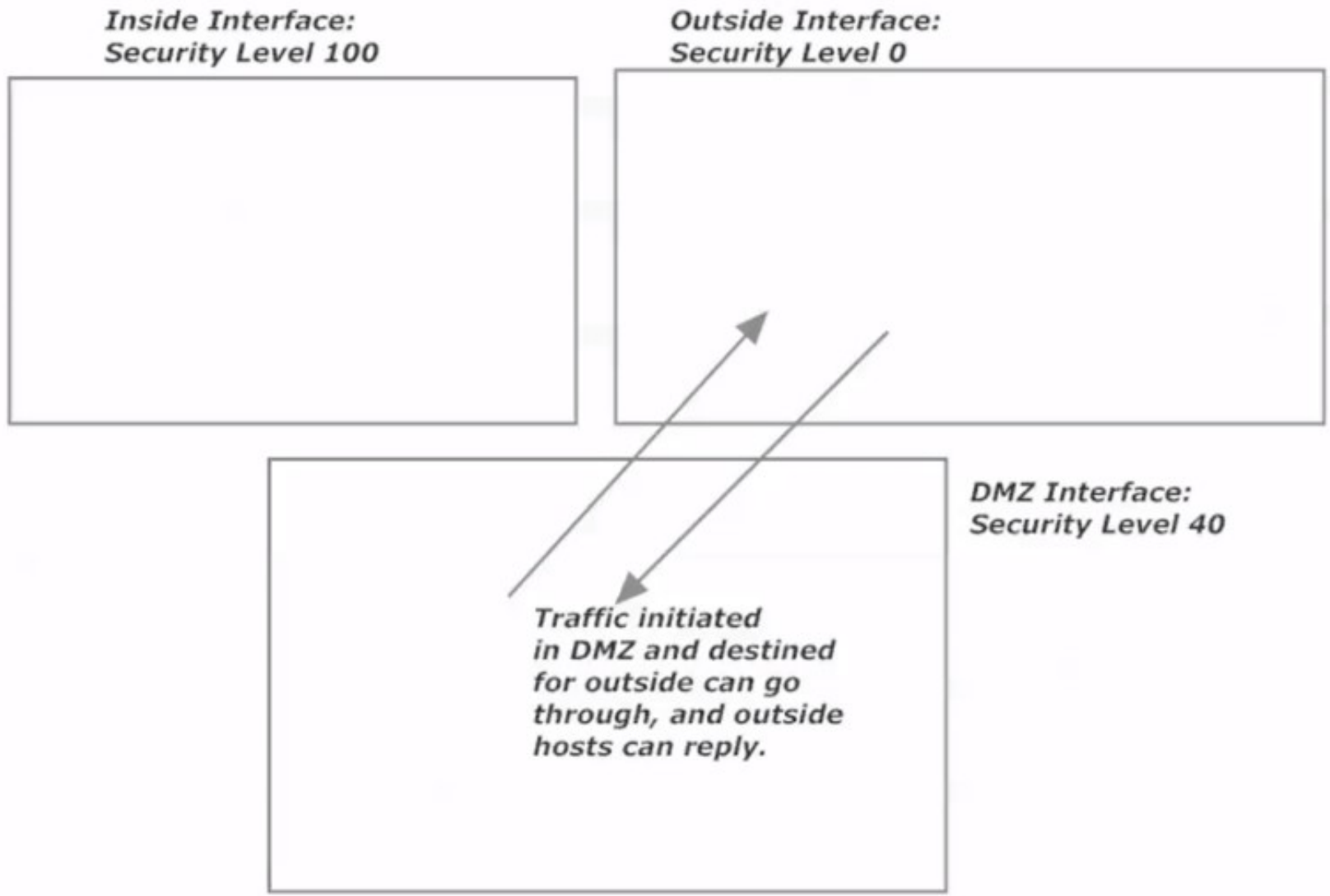
Niveles numéricos de seguridad

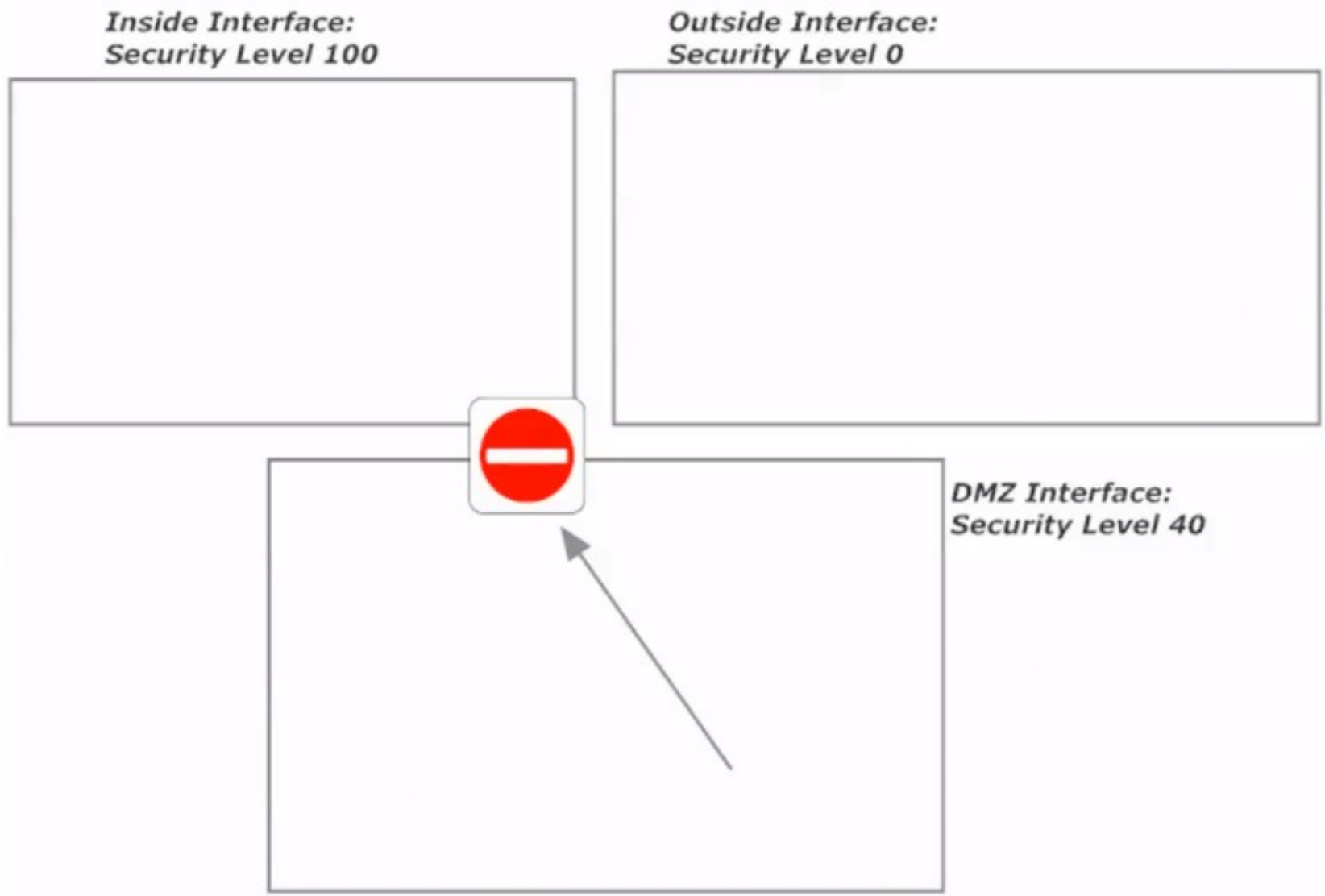
- Un nivel de seguridad de 1 a 99 siempre tiene dos ACL's implícitos:
  - Un ACL que permite el tráfico hacia un nivel de seguridad "lower-rated"
  - Un ACL que deniega el tráfico hacia un nivel "higher-rated"
- Un nivel de seguridad de 100 tiene un ACL implícito:
  - permit ip any any
- Un nivel de seguridad de 0 tiene un ACL implícito:
  - deny ip any any


Inside Interface:
Security Level 100
Outside Interface:
Security Level 0
Traffic Goes Through --
Higher to Lower Interface
Return Traffic Goes Through --
State Table Entry
DMZ Interface:
Security Level 40


Inside Interface:
Security Level 100
Outside Interface:
Security Level 0
Traffic Goes Through --
Higher to Lower Interface
Return Traffic Goes Through --
State Table Entry
DMZ Interface:
Security Level 40


Inside Interface:
Security Level 100
Outside Interface:
Security Level 0
No traffic initiated by outside hosts can go through, since the inside and DMZ interfaces have higher security levels.
DMZ Interface:
Security Level 40


Inside Interface:
Security Level 100
Outside Interface:
Security Level 0
DMZ Interface:
Security Level 40
Traffic initiated
in DMZ and destined
for outside can go
through, and outside
hosts can reply.


Inside Interface:
Security Level 100
Outside Interface:
Security Level 0
DMZ Interface:
Security Level 40

Configuración de interfaces

```
!
interface GigabitEthernet1/1
 shutdown
 nameif outside
 security-level 0
 no ip address
!
interface GigabitEthernet1/2
 shutdown
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet1/3
 shutdown
 no nameif
 no security-level
 no ip address
!
```

Configuración de interfaces

```
ciscoasa(config)# int gig 1/3
ciscoasa(config-if)# nameif?

interface mode commands/options:
  nameif
ciscoasa(config-if)# nameif ?

interface mode commands/options:
  WORD < 49 char  A name by which this interface will be referred in al
                  commands
ciscoasa(config-if)# nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 11.1.1.2 255.255.255.0
```

```
ciscoasa# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - B
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS le
       ia - IS-IS inter area, * - candidate default, U - per-user stati
       o - ODR, P - periodic downloaded static route, + - replicated ro
Gateway of last resort is not set

C        11.1.1.0 255.255.255.0 is directly connected, DMZ
L        11.1.1.2 255.255.255.255 is directly connected, DMZ
```

Next Generation Firewall (NGFW)

- Firewall de inspección de paquetes profundos que va más allá de la inspección y el bloqueo de puertos y protocolos para añadir inspección a nivel de aplicaciones, prevención de intrusiones e inteligencia desde el exterior del firewall.
- Un firewall “tradicional” provee stateful inspection del tráfico de red. Permite o bloquea en base a estado de conexión, puerto, red y protocolo.

Next Generation Firewall (NGFW)

Un NGFW puede contar con las siguientes funcionalidades:

- Capacidades de stateful inspection
- Intrusion prevention systems integrado (IPS)
- Inspección y control de aplicaciones para ver y bloquear aplicaciones riesgosas
- Threat intelligence sources
- Filtrado de URLs
- Bloqueo por geolocalización
- Consumo de listados de reputación a través de APIs.

Next Generation Firewall (NGFW)

Más funcionalidades…

- Filtrado por identidad (control de usuarios y grupos)
- Integración en modo transparente o nat-routed
- Inspección de tráfico cifrado (SSL, TLS, impacto en el performance).

Unified Threat Management (UTM)

Integran muchas funcionalidades de seguridad distintas en un solo appliance perimetral:

- Protección de correo electrónico (antispam)
- WAF (Web Application Firewall)
- Análisis de Malware por medio de sandbox
- Data Loss Prevention (DLP)

Tarea

- Hacer un ensayo sobre la evolución de los Web Application Firewalls (WAF) y su beneficio en las redes modernas y la nube.