Packet Tracer : Firewall i DMZ

Què és un Firewall? I una DMZ? Clica aquí.

Segmentació de la xarxa

La segmentació de xarxa amb un firewall és una tècnica de seguretat que consisteix a dividir una xarxa en múltiples segments o zones independents, cadascun amb el seu nivell de seguretat i polítiques d'accés específiques. L'objectiu és reduir la propagació d'amenaces i limitar l'accés només a les zones necessàries, la qual cosa disminueix la superfície d'atac.

Com es fa la segmentació amb un firewall?

- **Zones / segments / interfícies / VLAN:** S'estableixen zones (com ara Inside, Outside, DMZ, Guest).
- **Polítiques d'inspecció de trànsit**: Les polítiques de trànsit s'apliquen de manera predeterminada basant-se en els nivells de seguretat de les interfícies. Aquestes polítiques estableixen com s'ha de gestionar el trànsit entre zones sense necessitat d'una configuració específica.
- **Control de trànsit entre zones**: Es configuren regles que controlen el trànsit entre zones, com ara permetre el trànsit de la xarxa Inside a Outside, però no a la inversa, dependrà de la sensibilitat de les dades i el nivell de confiança. Els firewalls ASA (Adaptive Security Appliance) usen ACL (Access Control List).

Beneficis de la segmentació amb firewall

- Millora la seguretat limitant l'accés entre zones.
- Contenció de possibles amenaces: si una zona es compromet, el moviment lateral cap a altres zones està restringit.
- Control granular del trànsit: Permet definir polítiques específiques per cada zona segons les necessitats de seguretat.
- Aquesta tècnica és fonamental per a la seguretat de xarxes corporatives, especialment en entorns amb requisits de compliment normatiu i dades sensibles.

Nivells de seguretat

A Cisco ASA hi ha un sistema de nivells de seguretat per cada interfície, i aquests nivells determinen, per defecte, quin trànsit està permès i quin està denegat:

- Es pot enviar paquets a una xarxa amb un nivell de seguretat menor
- No es pot enviar paquets a una xarxa amb un nivell de seguretat major.
- Es pot rebre paquets des d'una xarxa amb un nivell de seguretat major.
- No es pot rebre paquets des d'una xarxa amb un nivell de seguretat menor.

Cada interfície es configura amb un nivell de seguretat que **oscil·la entre 0 i 100**, sent 100 la màxima i 0 la mínima.

ACL

Per defecte un firewall impedeix el pas de trànsit.
Una ACL és una eina que s'implementa principalment a firewalls i routers.
ACL permet definir regles per **permetre o denegar trànsit** cap a una xarxa o des d'una xarxa.

- Funcionament de les ACL

  Les ACLs funcionen mitjançant una sèrie de regles ordenades que especifiquen condicions permeses o denegades. Cada regla defineix criteris, com ara l'adreça IP d'origen i de destinació, els ports i el protocol. Aquestes condicions es comparen amb cada paquet de dades que travessa el dispositiu que implementa les ACL.

  Quan un paquet entra al dispositiu, revisa les ACLs per ordre fins que troba una regla que coincideixi amb les característiques del paquet. Si hi ha una coincidència, s'aplica l'acció associada amb la regla i el paquet s'accepta o es descarta segons correspongui. Si cap regla coincideix, s'aplica l'acció per defecte, denegar el trànsit.

- Exemple bàsic de regla ACL

  Sintaxi d'una regla ACL en un Firewall Cisco ASA:
  `access-list [nomACL] [acció] [protocol] [origen] [destí] [opcions]`

  `nomACL`: Nom que identifiqui l'ACL. Pots tenir múltiples regles dins de la mateixa ACL.
  `acció`: Pot ser **permit** (permetre el trànsit) o **deny** (bloquejar el trànsit).
  `protocol`: El protocol de xarxa: ip, tcp, udp, icmp, etc.
  `origen`: La IP d'origen i la seva màscara, si és una xarxa. S'usa **any** per indicar qualsevol adreça.
  `destí`: La IP de destí i la seva màscara, si és una xarxa. S'usa **any** per indicar qualsevol adreça.
  `opcions`: Generalment inclou el **port** o rangs de ports.

  Permetre trànsit HTTPS (port 443) des de la xarxa 192.168.1.0 a qualsevol xarxa:
  ```
  access-list EXEMPLE_ACL1 permit tcp 192.168.1.0 255.255.255.0 any eq 443
  ```

  Bloquejar trànsit cap a una IP (198.51.100.23) sospitosa a Internet:
  ```
  access-list EXEMPLE_ACL2 deny ip 192.168.1.0 255.255.255.0 host 198.51.100.23
  ```

- Aplicar la regla ACL

  Perquè la regla s'apliqui al trànsit, primer hem d'assignar la regla ACL a una interfície específica, la regla s'aplicarà al trànsit que passi per la interfície indicada.

  En un Firewall ASA es fa servir la següent sintaxi:
  access-group [nomACL] [direcció] interface [nomInterfície]

  nomACL: És el nom de la ACL que volem aplicar a la interfície. Aquesta ACL ja ha de ser definida prèviament amb access-list.
  direcció: Pot ser in o out.
  - **in** : Aplica l'ACL als paquets que entren des de la interfície.
  - **out** : Aplica l'ACL als paquets que surten del dispositiu per la interfície.

  nomInterfície: És el nom de la interfície a la qual volem aplicar la ACL (per exemple, inside, outside, GigabitEthernet0/1, etc.).

  Només permetre trànsit HTTPS (port 443) des de la xarxa 192.168.1.0 a qualsevol xarxa:
  ```
  access-group EXEMPLE_ACL1 in interface outside
  ```

  Això significa que qualsevol trànsit que entri a la ASA des de la interfície outside es comprovarà contra les regles de l'ACL «EXEMPLE_ACL1». Només es permetrà el trànsit que compleixi les condicions especificades a l'ACL (trànsit HTTPS provinent de la xarxa 192.168.1.0/24), i la resta serà bloquejat.

- Utilitat de les ACLs

  Les ACLs són fonamentals per a la seguretat de xarxes, ja que permeten definir qui pot accedir a quins recursos i amb quins permisos. En un ASA, les ACLs es fan servir per filtrar el trànsit i protegir xarxes contra accés no autoritzat i potencials amenaces.

Polítiques d’inspecció de trànsit

Analitzen i controlen el trànsit de xarxa per aplicar normes de seguretat, permetent o bloquejant trànsit. En aquesta pràctica, ens enfocarem específicament a acceptar de forma controlada l'accés de paquets depenent del seu protocol.

Cadena de comandes per crear i aplicar una política:

class-map: Has de definir un nom pel grup de trànsit.
match: Especifica criteris d’inspecció dins del class-map.

policy-map: Has de definir un nom per la política.
class: Especifica el class-map a usar a la policy-map.
inspect: Acció dins del policy-map pel control del trànsit. Donem accés, prèvia inspecció, a un protocol.

service-policy: Escull el policy-map i a quina interfície s’aplica, amb aquesta instrucció s’aplica tota la configuració al trànsit real.

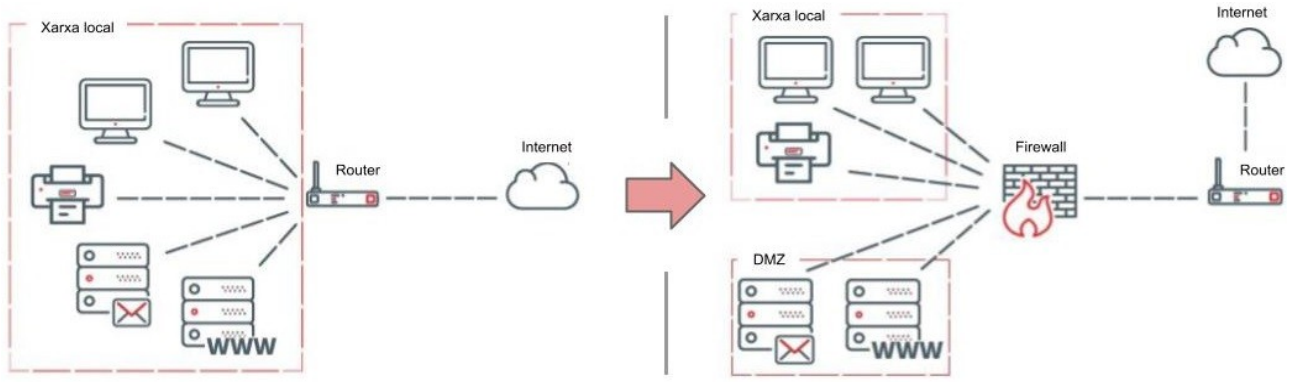
Les tres comandes principals (class-map , policy-map , service-policy) s’han d’iniciar des de la terminal de configuració base, introdueix «exit» quan finalitzis cada cadena de comandes.

- Exemple de definició de grup de trànsit:
```
ciscoasa(config)#class-map EXEMPLE_CLASSE_TRAFIC
ciscoasa(config-cmap)#match default-inspection-traffic
```
- Premem «exit» per tornar al mode configuració base i poder crear, per exemple, una política:
```
ciscoasa(config-cmap)#exit
ciscoasa(config)#
```

En els dispositius Cisco en mode configuració pots usar «?» per veure les opcions de compleció de la comanda.

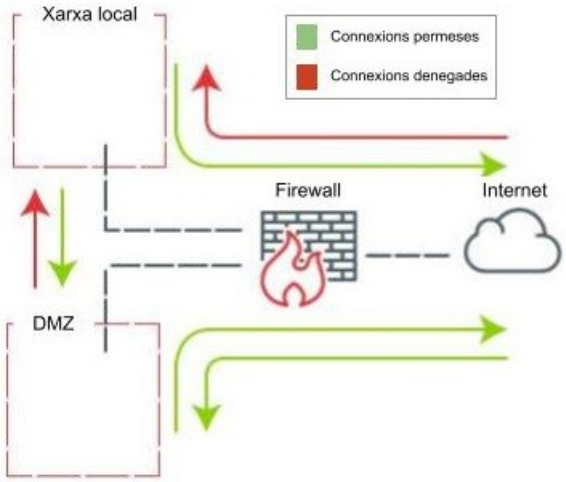
Disseny de la DMZ

Quan es permet l'accés des d'Internet a un servidor, augmenta el risc de patir un incident de seguretat. Si un ciberdelinqüent aconsegueix vulnerar la seguretat del servidor, podria comprometre la resta de dispositius connectats a la xarxa, fins i tot aquells que no són accessibles des d'Internet. Un accés no desitjat podria derivar en una infecció per ransomware, comunicacions espiades, fitxers robats, caigudes de servei, etc.



Per minimitzar els riscos derivats d'un servidor amb accés des d'Internet que pogués comprometre la seguretat de l'organització, s'ha d'utilitzar un firewall i una xarxa local anomenada zona desmilitaritzada (DMZ).

La configuració stàndard d'un firewall amb DMZ és la següent:



Màxima seguretat a la xarxa local: Tot trànsit d'entrada és denegat i el de sortida és permès.

Mínima seguretat a la xarxa d'Internet, de manera que totes les xarxes locals hi poden accedir però no a la inversa.

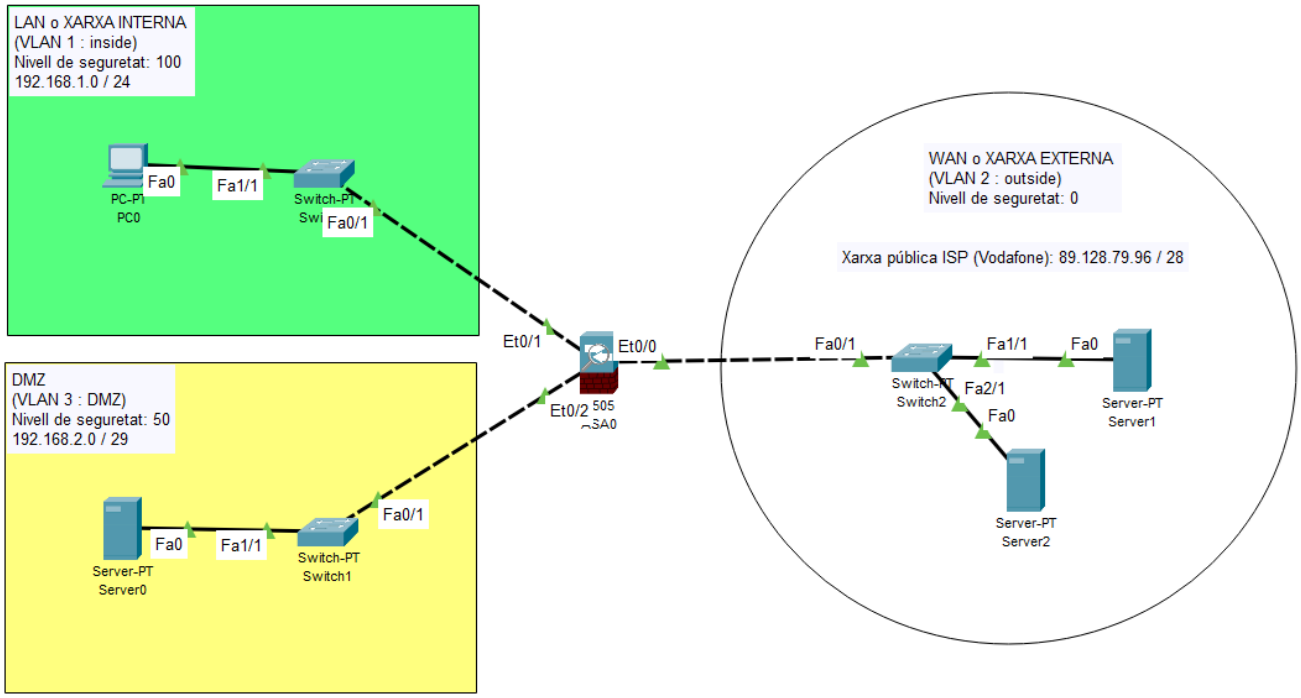
Mitjana seguretat a la DMZ, pot accedir a Internet però no a la xarxa local. Des d'Internet no s'hi pot accedir per defecte, òbviament sí s'ha de permetre l'entrada ja que el que volem es donar accés a un servidor, necessitem establir regles d'accés específiques.

ACTIVITATS

Implementació d'un Firewall i DMZ

L'empresa Embotits<XYZ> ens contracta perquè implementem una xarxa segura que inclogui un servidor web.
(Substitueix X per la inicial del teu nom, Y per la del primer cognom i Z per la del segon)

Configurarem 3 interfícies pel firewall, cada interfície estarà assignada a una VLAN.
Crearem 3 zones: **DMZ**, **inside**, i **outside** en un firewall **Cisco ASA**. El disseny segueix els principis habituals de segmentació i seguretat per protegir la xarxa interna (Inside) i limitar l'accés a la zona pública (DMZ) des de fora (outside). Aquí tens l'esquema de seguretat de la xarxa:



Topologia

- **inside**: Xarxa privada segura (**192.168.1.0/24**)
  - L'ordinador obtindrà la IP dinàmicament del **servidor DHCP** del firewall. Aquesta és la configuració del firewall que indica que implementa DHCP pels terminals que es connectin a la xarxa inside, i el rang d'IPs que ofereix:

```
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
```

- **DMZ**: Xarxa separada per serveis públics (**192.168.2.0/29**)
  - Per qüestions de seguretat volem restringir el nombre de dispositius públics, només hi poden haver 6 dispositius a la xarxa.
  - Assigna la última IP disponible per dispositius al servidor web.
- **outside**: Xarxa pública o internet (Amb IP pública)
  - Utilitzarem la xarxa pública assignada pel nostre ISP (Internet Service Provider), Vodafone: **89.128.79.96 / 28**.
  - Reservarem la primera IP disponible pel default gateway.

- Dins d’aquesta xarxa configurarem dos servidors HTTP per realitzar les proves, els hi assignarem la segon i tercera IP disponibles.
- En un entorn real, faria falta utilitzar NAT (Network Address Translation) per permetre que els dispositius de la xarxa interna accedeixin a Internet a través de les IPs públiques assignades per l'ISP.

Principis de Seguretat

1. Permetre accés limitat des de Outside a la DMZ: Només pels serveis públics HTTP i HTTPS.
2. Permetre accés des de Inside a la DMZ: Accés complet per manteniment i gestió de serveis.
3. Permetre accés des de Inside a Outside: Per navegar per internet o accedir a recursos externs.
4. Denegar la resta del trànsit no definit: Política de seguretat per defecte de "denegar tot".

Passos a seguir en la configuració

1. Muntarem un firewall ASA 5505.
2. Tingues en compte que per configurar el firewall primer has de tenir permisos de configuració:

```
ciscoasa>enable
Password:
ciscoasa#configure terminal
ciscoasa(config)#
```

3. Per defecte el firewall no té password, li assignarem el password «ciscoasa».
4. Canviem el nom del firewall per Embotits<XYZ>fw.
5. Canviem el nom del domini per Embotits<XYZ>.cat.
6. Muntarem la resta dels dispositius de xarxa i els terminals i els unirem amb el cablejat indicat: Directe per dispositius diferents i creuat per dispositius similars.
7. El firewall ASA 5505 inclou dues VLAN per defecte:
8. Ens assegurem que la xarxa interna utilitza la VLAN 1, anomenada inside, que per defecte té un nivell de seguretat de 100.
9. Internet ha d'usar VLAN 2, outside, nivell de seguretat 0.
10. Creem la interfície DMZ: Per termes de llicència ens impedirà fer una nova xarxa que pugui comunicar-se amb VLAN 1, per solucionar-ho denegarem el tràfic cap a la xarxa interna amb:

```
no forward interface vlan 1
```

11. Assignarem a les interfícies del firewall les IP corresponents.
12. Assignarem IP als terminals.
13. Un cop finalitzada la configuració, per cada terminal, comprovem que efectivament tenim connectivitat amb el default gateway de la seva xarxa fent ping.
14. En aquest punt no podem enviar paquets entre les xarxes: Tot està restringit per defecte. Hem de crear polítiques d'inspecció de trànsit per permetre el protocol icmp i http. Un cop fet ja tindrem el comportament normal.
15. Valida que podem accedir o no a les zones depenent del nivell de seguretat, es a dir: Podem accedir des LAN i DMZ a WAN, i també des de LAN a DMZ, hem corregit la restricció per llicència.
16. Ara volem que es pugui accedir des d'outside al servidor web de la DMZ: Usem ACL.
17. Comprovem la configuració: Des dels terminals d'outside, intenta fer un ping i veure la pàgina principal del servidor web a la DMZ.

Comandes rellevants per interactuar amb el firewall

Configuració del dispositiu:
show running-config

Configuració de les interfícies:
show interface ip brief

IPs de les xarxes:
show route

VLANs i a quina interfície estan assignades:
show switch vlan

ACL configurades:
show access-list

Guarda la configuració en memòria no volàtil:
write memory

Esborrar instrucció:
no <instrucció a eliminar>

Canviar password:
enable password <password>

Configurar nom del domini:
domain-name <nom del domini>

configurar IP de VLAN:
interface <nom VLAN>
ip address <ip address> <subnet mask>

Creació d'una VLAN i assignar a una interfície física :
interface <nom de la interfície>
nameif <nom de la VLAN a crear>
ip address <ip default gateway> <subnet mask>
security-level <nivell de seguretat>
no shutdown

```
ciscoasa(config)#interface GigabitEthernet1/1
ciscoasa(config-if)#nameif Inside
ciscoasa(config-if)#ip address 192.168.100.10 255.255.255.0
ciscoasa(config-if)#security-level 90
ciscoasa(config-if)#no shutdown
```

Assignar vlan concreta a un port via comandes:
interface <nomdela interficie>
switchport access vlan <numero de VLAN>

BIBLIOGRAFIA I WEBGRAFIA

«Cisco». https://www.cisco.com/c/es_mx/support/docs/security/asa-5500-x-series-next-generation-firewalls/115904-asa-config-dmz-00.html
«incibe». https://www.incibe.es/empresas/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa
«itexamanswers». https://itexamanswers.net/9-3-1-1-packet-tracer-configuring-asa-basic-settings-firewall-using-cli-answers.html

---