

# Migració de la infraestructura de seguretat perimetral per a

TecnoCampus

La informació continguda en aquest document pot ser de caràcter privilegiat y/o confidencial. Qualsevol disseminació, distribució o còpia d'aquest document per qualsevol altra persona diferent als receptors originals queda estrictament prohibida. Si ha rebut aquest document per error, sis plau notifiqueu immediatament al emissor i esborri qualsevol còpia d'aquest document.

# Migració de la infraestructura de seguretat perimetral

## Índex

<b>1. INTRODUCCIÓ.....</b>	<b>3</b>
1.1. DESCRIPCIÓ .....	3
1.2. OBJECTIUS.....	3
1.3. DESCRIPCIÓ GENERAL DE LES INFRAESTRUCTURES .....	4
<b>2. CONFIGURACIÓ DEL DISPOSITIU.....</b>	<b>5</b>
2.1. DISPOSITIU .....	5
2.2. CREDENCIALS D'ACCÉS.....	5
2.3. GENERAL.....	5
2.4. INTERFÍCIES .....	5
2.5. TAULA D'ENRUTAMENT .....	6
2.6. OBJECTES ADRECES DEL FIREWALL.....	6
2.7. OBJECTES SERVEIS .....	7
2.8. NATS D'ENTRADA (VIRTUAL IPS) .....	9
2.9. POLÍTIQUES DE FIREWALL .....	10
2.10. SERVEI ANTIVIRUS.....	11
2.11. SERVEI DE FILTRAGE WEB .....	11
2.12. SERVEI APPLICATION CONTROL.....	11
2.13. SERVEI INTRUSION PROTECTION.....	11

# 1. Introducció

## 1.1. Descripció

El present document descriu la configuració realitzada en el dispositiu Fortigate-80D de Fortinet a la empresa TecnoCampus resultat de la substitució de un Firewall perimetral Cisco de l'organització.

## 1.2. Objectius

El objectiu d'aquest document és la de formalitzar el traspàs d'informació al equip tècnic responsable del manteniment de les infraestructures instal·lades. Aquesta informació fa referencia al disseny, instal·lació i configuració dels dispositius i sistemes afectats per la implementació.

La present documentació inclou:

- Descripció general de les infraestructures instal·lades.
- Polítiques de filtratge de tràfic.
- Perfils de seguretat.
- Connexions Túnel.

### 1.3. Descripció general de les infraestructures

Actualment la infraestructura té la següent distribució:

En aquest esquema es pot veure com el firewall disposa actualment de dos connexions a internet (Port1 i Port4) que es connecten a través de diferents routers.

La infraestructura disposa de dos xarxes locals, la xarxa de servidors i la xarxa d'estacions de treball.

## 2. Configuració del Dispositiu

A continuació es detalla la configuració del dispositiu Fortigate-80D.

### 2.1. Dispositiu

Header 1	Header 2	Header 3
Row 1, Col 1	Row 1, Col 2	Row 1, Col 3
Row 2, Col 1	Row 2, Col 2	Row 2, Col 3
Row 3, Col 1	Row 3, Col 2	Row 3, Col 3

### 2.2. Credencials d'accés

Accés: <https://10.132.4.254:8443>

Usuari: admin

Password: dfAS34

Restriccions d'accés: xarxes 10.132.4.0/24, 10.132.6.0/24, 218.142.21.231/32

### 2.3. General

El dispositiu està configurat en mode NAT, és a dir, es separen diverses xarxes a nivell tres d'enrutament.

DNS:

- Servidor Primari: 10.132.6.96
- Servidor Secundari: 201.91.101.23
- Non del domini Local: entenca.br.respes.es

### 2.4. Interfícies [#config system interface]

El dispositiu instal·lat disposa d'una taula de polítiques de connexió per tal de definir el comportament del mateix per cada una de les connexions tractades.

Header 1	Header 2	Header 3
Row 1, Col 1	Row 1, Col 2	Row 1, Col 3
Row 2, Col 1	Row 2, Col 2	Row 2, Col 3
Row 3, Col 1	Row 3, Col 2	Row 3, Col 3

## 2.5. Taula d'enrutament [#config router static]

S'ha definit 2 default gw per permetre la sortida per les dues sortides a internet de la organització. Per defecte el tràfic sortirà a través del GW 10.132.0.1 (prioritat menor) i en cas de caiguda de la línia es redirigirà el tràfic a través del GW 10.132.7.1.

Header 1	Header 2	Header 3
Row 1, Col 1	Row 1, Col 2	Row 1, Col 3
Row 2, Col 1	Row 2, Col 2	Row 2, Col 3
Row 3, Col 1	Row 3, Col 2	Row 3, Col 3

S'ha definit una sèrie de Health-checks de ping [config System link-monitor] a través de les interfícies wan per detectar la caiguda de les línies de comunicacions.

## 2.6. Objectes Adreces del Firewall [#config firewall address]

El dispositiu actualment te vinculats determinats objectes (noms descriptius) a adreces IP per tal de facilitar la seva utilització en el sistema.

Header 1	Header 2	Header 3
Row 1, Col 1	Row 1, Col 2	Row 1, Col 3
Row 2, Col 1	Row 2, Col 2	Row 2, Col 3
Row 3, Col 1	Row 3, Col 2	Row 3, Col 3

## 2.7. Objectes Serveis [#config firewall service custom]

El dispositiu configurat disposa de serveis predeterminats per defecte establerts per FortiNet i addicionalment te introduïts serveis personalitzats.

Els serveis predeterminats són:

Header 1	Header 2	Header 3
Row 1, Col 1	Row 1, Col 2	Row 1, Col 3
Row 2, Col 1	Row 2, Col 2	Row 2, Col 3
Row 3, Col 1	Row 3, Col 2	Row 3, Col 3



Header 1	Header 2	Header 3
Row 1, Col 1	Row 1, Col 2	Row 1, Col 3
Row 2, Col 1	Row 2, Col 2	Row 2, Col 3
Row 3, Col 1	Row 3, Col 2	Row 3, Col 3

Els serveis addicionals són:

Header 1	Header 2	Header 3
Row 1, Col 1	Row 1, Col 2	Row 1, Col 3
Row 2, Col 1	Row 2, Col 2	Row 2, Col 3
Row 3, Col 1	Row 3, Col 2	Row 3, Col 3

## 2.8. NATs d'entrada (Virtual IPs) [#config firewall vip]

S'ha definit els següents NATs d'entrada (VIPs en nomenclatura Fortinet)

Header 1	Header 2	Header 3
Row 1, Col 1	Row 1, Col 2	Row 1, Col 3
Row 2, Col 1	Row 2, Col 2	Row 2, Col 3
Row 3, Col 1	Row 3, Col 2	Row 3, Col 3

## 2.9. Polítiques de Firewall [#config firewall policy]

A continuació es mostren les polítiques de filtratge definides en el dispositiu Fortigate:

Header 1	Header 2	Header 3
Row 1, Col 1	Row 1, Col 2	Row 1, Col 3
Row 2, Col 1	Row 2, Col 2	Row 2, Col 3
Row 3, Col 1	Row 3, Col 2	Row 3, Col 3

## 2.10. Servei Antivirus

El servei antivirus perimetral proveeix d'una base de dades automatitzada per assegurar la protecció davant de possible contingut de malware detectat a través de la navegació WEB. Actualment el dispositiu té com el perfil d'antivirus activat UTM-AV que detecta i neteja malware i possibles connexions a xarxes de Botnets.

## 2.11. Servei de Filtrage Web

El servei de filtratge de web, proveeix d'un servei de filtratge de contingut web a través dels protocols de navegació.

Actualment en el dispositiu s'ha definit el perfil UTM-WF que actualment únicament genera logs de tot el tràfic de navegació web.

## 2.12. Servei Application control

El servei de Application Control realitza un filtratge a nivell d'aplicació per tal de bloquejar o filtrar determinades comunicacions d'aplicacions.

En el dispositiu s'ha activat el perfil UTM-APP i s'ha configurat per a generar logs de totes les aplicacions utilitzades i bloqueja totes les connexions d'aplicacions típiques de BotNets.

## 2.13. Servei Intrusion Protection

El Servei de Intrusion Protection permet detectar possibles atacs de xarxa contra la infraestructura de la organització.

En el dispositiu s'ha activat el perfil UTM-IPS en les polítiques de navegació web i s'han activat el comportament per defecte (bloqueig en cas necessari o monitorzació) de les signatures de tipus IPSLOC, de criticitat "high" que afectin a serveis de sistemes operatius Windows.