

Migració de la infraestructura de seguretat perimetral per a

Innevis 2000

Desembre, 2015

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

**Índex**

[1. Introducció 3](#_Toc439936325)

[1.1. Descripció 3](#_Toc439936326)

[1.2. Objectius 3](#_Toc439936327)

[1.3. Descripció general de les infraestructures 4](#_Toc439936328)

[2. Configuració del Dispositiu 5](#_Toc439936329)

[2.1. Dispositiu 5](#_Toc439936330)

[2.2. Credencials d’accés 5](#_Toc439936331)

[2.3. General 5](#_Toc439936332)

[2.4. Interfícies .................. 5](#_Toc439936333)

[*2.5.* Taula d’enrutament ............................ 6](#_Toc439936334)

[2.6. Objectes Adreces del Firewall ...................................................... 6](#_Toc439936335)

[2.7. Objectes Serveis …………………………………………………………………………………………….7](#_Toc439936336)

[2.8. NATs d’entrada (Virtual IPs) ……………………………………………………………………………..9](#_Toc439936337)

[2.9. Polítiques de Firewall ..................................................................... 10](#_Toc439936338)

[2.10. Servei Antivirus 11](#_Toc439936339)

[2.11. Servei de Filtrage Web 11](#_Toc439936340)

[2.12. Servei Application control 11](#_Toc439936341)

[2.13. Servei Intrusion Protection 11](#_Toc439936342)

1. Introducció

## Descripció

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

## Objectius

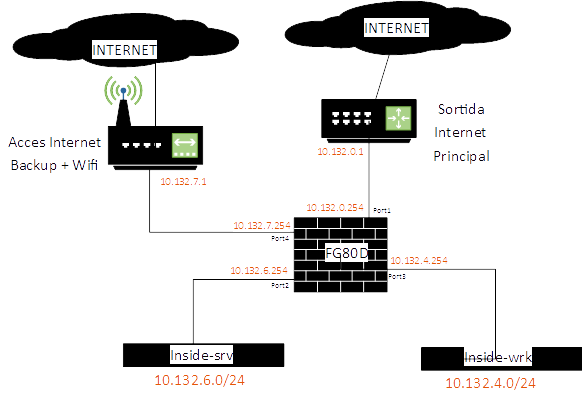
El objectiu d’aquest document és la de formalitzar el traspàs d’informació al equip tècnic responsable del manteniment de les infraestructures instal·lades. Aquesta informació fa referencia al disseny, instal·lació i configuració dels dispositius i sistemes afectats per la implementació.

La present documentació inclou:

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

## Descripció general de les infraestructures

Actualment la infraestructura te 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.

1. Configuració del Dispositiu

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

## Dispositiu

|  |  |
| --- | --- |
| Marca-Model | FortiGate 80D *[config-version]* |
| OS/Firmware | v5.0.2,build642 (141118) *[config-version]* |
| S/N |  |

## 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

## General

El dispositiu està configurat en mode NAT, és a dir, es separen vàries 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

## 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.

|  |  |  |  |
| --- | --- | --- | --- |
| Interficie  *[edit]* | Alias  *[set alias]* | Address/FQDN  *[set ip]* | DHCPRelay  *[set dhcp-relay-ip]* |
| Port1 | Outside | 10.132.0.254/24 | - |
| Port2 | Inside-srv | 10.132.6.254/24 | - |
| Port3 | Inside-wrk | 10.132.4.254/24 | 10.132.6.96 |
| Port4 | Outside-wlan | 10.132.7.254/24 | - |

## 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.

|  |  |  |  |
| --- | --- | --- | --- |
| Xarxa Destí | GW  *[set Gateway]* | Interficie  *[set device]* | Prioritat  *[set priority]* |
| 0.0.0.0/0.0.0.0 | 10.132.0.1 | Port1 | 10 |
| 0.0.0.0/0.0.0.0 | 10.132.7.1 | Port4 | 20 |

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.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Servidor Destí  *[set server]* | GW  *[set Gateway-ip]* | Interficie  *[set srcintf]* | Interval  *[set interval]* | failtime  *[set failtime]* | recovery  *[set recoverytime]* |
| 8.8.4.4 | 10.132.0.1 | Port1 | 3 | 3 | 3 |
| 8.8.4.4 | 10.132.7.1 | Port4 | 3 | 3 | 3 |

## 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name  *[edit]* | Category | Address/FQDN  *[set subnet]* | Interface | Type\*  *[set type]* |
| Inside\_srv | Address | 10.132.6.0/255.255.255.0 | Any | Subnet |
| Inside\_wrk | Address | 10.132.4.0/255.255.255.0 | Any | Subnet |
| Cloud1 | Address | 5.125.205.142/255.255.255.224 | Any | Subnet |
| Cloud2 | Address | 91.117.121.65/255.255.255.240 | Any | Subnet |
| Srv-demeter | Address | 10.132.6.62 | Any | Subnet |
| Srv-devrepo | Address | 10.132.6.97 | Any | Subnet |
| Srv-nebulaz | Address | 10.132.6.96 | Any | Subnet |
| Vpn-net | Address | 10.10.10.100.10.10.10.150 | Any | Range |

*\*[set type] = not exist (Subnet) / [set type] = iprange (range)*

## 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:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nom del Servei  *[edit]* | Categoria  *[set category]* | Ports TCP  *[set tcp-portrange]* | Ports UDP  *[set udp-portrange]* | Protocol  *[set protocol]* |
| ALL | General |  |  | IP |
| ALL\_TCP | General | 1-65535 |  |  |
| ALL\_UDP | General | 0 | 1-65535 |  |
| ALL\_ICMP | General |  |  | ICMP |
| ALL\_ICMP6 | General |  |  | ICMP6 |
| GRE | Tunneling |  |  | IP |
| AH | Tunneling |  |  | IP |
| ESP | Tunneling |  |  | IP |
| AOL |  | 5190-5194 |  |  |
| BGP | Network Services | 179 |  |  |
| DHCP | Network Services | 0 | 67-68 |  |
| DNS | Network Services | 53 | 53 |  |
| FINGER |  | 79 |  |  |
| FTP | File Access | 21 |  |  |
| FTP\_GET | File Access | 21 |  |  |
| FTP\_PUT | File Access | 21 |  |  |
| GOPHER |  | 70 |  |  |
| H323 | VoIP, Messaging & Other Applications | 1720 1503 | 1719 |  |
| HTTP | Web Access | 80 |  |  |
| IKE | Tunneling | 0 | 500 4500 |  |
| IMAP | Email | 143 |  |  |
| IMAPS | Email | 993 |  |  |
| Internet-Locator-Service |  | 389 |  |  |
| IRC | VoIP, Messaging & Other Applications | 6660-6669 |  |  |
| L2TP | Tunneling | 1701 | 1701 |  |
| LDAp | Authentication | 389 |  |  |
| NetMeeting |  | 1720 |  |  |
| NFS | File Access | 111 2049 | 111 2049 |  |
| NNTP | Network Services | 123 | 123 |  |
| OSPF | Network Services |  |  | IP |
| PC-Anywhere | Remote Access | 5631 | 5632 |  |
| PING | Network Services |  |  | ICMP |
| TIMESTAMP |  |  |  | ICMP |
| INFO\_REQUEST |  |  |  | ICMP |
| INFO\_ADDRESS |  |  |  | ICMP |
| ONC\_RPC | Remote Access | 111 | 111 |  |
| DCE\_RPC | Remote Access | 135 | 135 |  |
| POP3 | Email | 110 |  |  |
| POP3S | Email | 995 |  |  |
| PPTP | Tunneling | 1723 |  |  |
| QUAKE |  | 0 | 26000 27000 27910 27960 |  |
| RAUDIO |  | 0 | 7070 |  |
| REXEC |  | 512 |  |  |
| RIP | Network Services | 0 | 520 |  |
| RLOGIN |  | 513:512-1023 |  |  |
| RSH |  | 514:512-2013 |  |  |
| SCCP | VoIP, Messaging & Other Applications | 2000 |  |  |
| SIP | VoIP, Messaging & Other Applications | 5060 | 5069 |  |
| SIP-MSNmessenger | VoIP, Messaging & Other Applications | 1863 |  |  |
| SAMBA | File Access | 139 |  |  |
| SMTP | Email | 25 |  |  |
| SMTPS | Email | 465 |  |  |
| SNMP | Network Services | 161-162 | 161-162 |  |
| SSH | Remote Access | 22 |  |  |
| SYSLOG | Network Services | 0 | 514 |  |
| TALK |  | 0 | 517-518 |  |
| TELNET | Remote Access | 23 |  |  |
| TFTP | File Access | 0 | 69 |  |
| MGCP |  | 0 | 2427 2727 |  |
| UUCP |  | 540 |  |  |
| VDOLIVE |  | 7000-7010 |  |  |
| WAIS |  | 210 |  |  |
| WINFRAME |  | 1494 2598 |  |  |
| X-WINDOWS | Remote Access | 6000-6063 |  |  |
| PING6 |  |  |  | ICMP6 |
| MS\_SQL | VoIP, Messaging & Other Applications | 1433 1434 |  |  |
| MYSQL | VoIP, Messaging & Other Applications | 3306 |  |  |
| RDP | Remote Access | 3389 |  |  |
| VNC | Remote Access | 5900 |  |  |
| DHCP6 | Network Services | 0 | 546 547 |  |
| SQUID | Tunneling | 3128 |  |  |
| SOCKS | Tunneling | 1080 | 1080 |  |
| WINS | Remote Access | 1512 | 1512 |  |
| RADIUS | Authentication | 0 | 1812 1813 |  |
| RADIUS-OLD |  | 0 | 1645 1646 |  |
| CVSPSERVER |  | 2401 | 2401 |  |
| AFS3 | File Access | 7000-7009 | 7000-7009 |  |
| TRACEROUTE | Network Services | 0 | 33434-33535 |  |
| RTSP | VoIP, Messaging & Other Applications | 554 7070 8554 | 554 |  |
| MMS |  | 1755 | 1024-5000 |  |
| KERBEROS | Authentication | 88 | 88 |  |
| LDAP\_UDP | Authentication | 0 | 389 |  |
| SMB | File Access | 445 |  |  |
| NONE |  |  |  |  |
| webproxy | Web Proxy | 0-65535:0-65535 |  | ALL |

Els serveis addicionals són:

|  |  |  |  |
| --- | --- | --- | --- |
| Nom del Servei  *[edit]* | Categoria | Ports TCP  *[set tcp-portrange]* | Ports UDP  *[set udp-portrange]* |
| 43421\_UDP | Uncategorized | 0 | 43421 |
| 8083\_TCP | Uncategorized | 8083 |  |

## NATs d’entrada (Virtual IPs) *[#config firewall vip]*

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name  *[edit]* | External IP Address/Range  *[set extintf] / [set extip]* | External Service Port  *[set extport ]/[set protocol]* | Mapped IP Address/Range  *[set mappedip]* | Map to Port  [set mappedport]/ *[set protocol]* |
| VIP\_srv-01 | Port1/10.132.0.254 | 43421/udp | 10.132.6.62 | 43421/udp |
| VIP\_srv-02 | Port1/10.132.0.254 | 8083/tcp | 10.132.6.97 | 8083/tcp |

## Polítiques de Firewall *[#config firewall policy]*

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | From  *[set srcintf] / [set srcaddr]* | To  *[set dstintf] / [set dstaddr]* | Source  *[set srcaddr]([set groups])* | Destination  *[set dstaddr]* | Service  *[set service]* | Action  *[set action]* | AV  *[set av-profile]* | Web Filter  *[set webfilter-profile]* | App Control  *[set application-list]* | IPS  *[set ips-sensor]* | SSL Inspect  *[set ssl-ssh-profile]* | Log  *[set logtraffic]* | NAT  *[set nat]* |
| 1 | Port3(Inside-wrk) | Port4(Outside-wlan) | Inside\_wrk | All | ALL | Accept | UTM-AV | UTM-WF | UTM-APP | UTM-IPS | Cert. | All | Enable |
| 2 | Port3(Inside-wrk) | Port2(Inside-srv | Inside\_wrk | Inside\_srv | ALL | Accept |  |  |  |  |  | disable |  |
| 3 | Port2(Inside-srv) | Port3(Inside-wrk) | Inside\_srv | Inside\_wrk | ALL | Accept |  |  |  |  |  | disable |  |
| 4 | Port3(Inside-wrk) | Port1(Outside) | Inside\_wrk | All | ALL | Accept | UTM-AV | UTM-WF | UTM-APP | UTM-IPS | Cert. | All | Enable |
| 5 | Port2(Inside-srv) | Port1(Outside) | Inside\_srv | All | ALL | Accept | UTM-AV | UTM-WF | UTM-APP | UTM-IPS | Cert. | All | Enable |
| 6 | Port2(Inside-srv) | Port4(Outside-wlan) | Inside\_srv | All | ALL | Accept | UTM-AV | UTM-WF | UTM-APP | UTM-IPS | Cert. | All | Enable |
| 7 | Ssl.root | Port2(Inside-srv) | Vpn-net (Global | Inside\_srv | ALL | Accept |  |  |  |  |  | All | Enable |
| 8 | Ssl.root | Port4(Inside-wrk) | Vpn-net (Global) | Inside\_wrk | ALL | Accept |  |  |  |  |  | All | Enable |
| 9 | Port1(Outside) | Port2(Inside-srv) | Cloud1  Cloud2 | VIP-srv-01 | 8083\_TCP | Accept |  |  |  |  |  | All |  |
|  | Any | Any | All | All | ALL | Deny |  |  |  |  |  |  |  |

## Servei Antivirus*[#config antivirus profile]*

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 te com el perfil d’antivirus activat **UTM-AV** ***[edit]***que detecta i neteja malware i possibles connexions a xarxes de Botnets.

## Servei de Filtrage Web*[#config webfilter profile]*

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 *[edit]*** que actualment únicament genera logs de tot el tràfic de navegació web.

## Servei Application control*[#config application list]*

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*[edit]*** i s’ha configurat per a generar logs de totes les aplicacions utilitzades i bloqueja totes les connexions d’aplicacions típiques de BotNets.

## Servei Intrusion Protection *[#config ips sensor]*

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

En el dispositiu s’ha activa el perfil **UTM-IPS** ***[edit]***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 client***[set location]***, de criticitat “critical” ***[set severity]*** i “high” ***[set severity]*** que afectin a serveis de sistemes operatius Windows, Linux i MacOS***[set os]***.