Migració de la infraestructura de seguretat perimetral per a TecnoCampus

Gener 2019

Índex

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

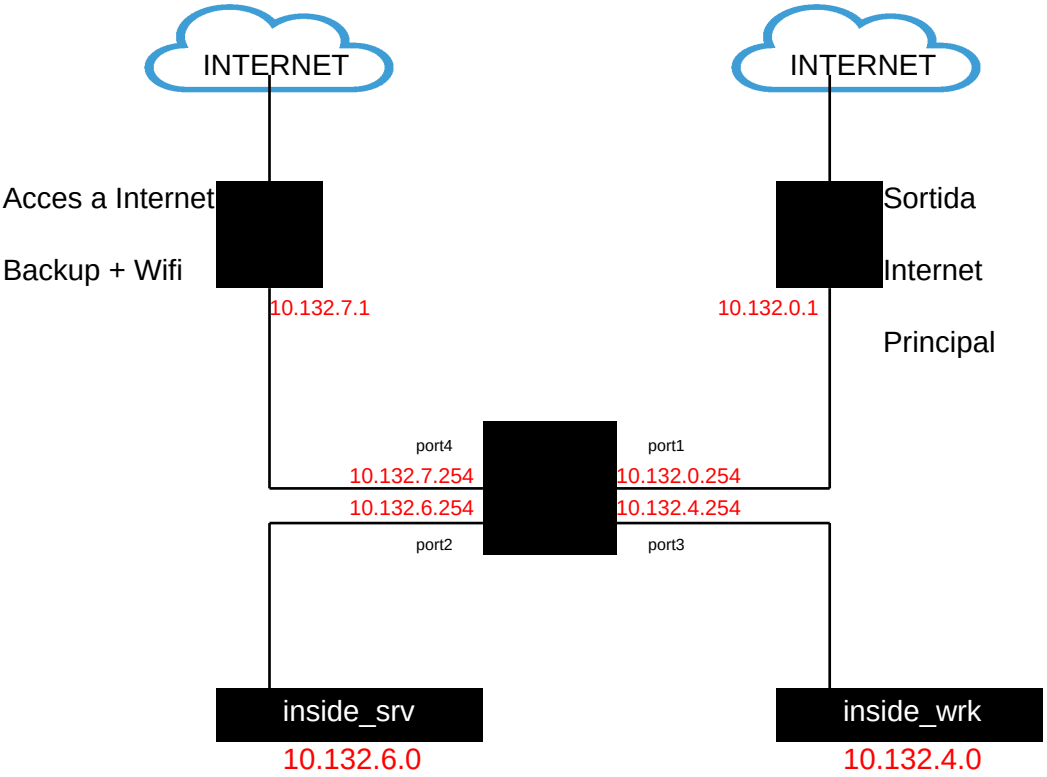
El objectiu d'aquest document és la de formalitzar el traspàs d'informació al equip tècnic responsable del manteniment de les infraestructures instal·lades. Aquesta informació fa referencia al disseny, instal·lació i configuració dels dispositius i sistemes afectats per la implementació.

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 te la següent distribució:



En aquest esquema es pot veure com el firewall disposa actualment de dos conexions 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

Marca-Model	Fortigate 80D
OS/Firmware	5.02
S/N	

2.2. Credencials d'accés

Accés: https://10.132.4.254:8443

Usuari: admin

Password: dfAS34

Restriccions d'accés: xarxes 10.132.4.0 255.255.255.0, 10.132.6.0 255.255.255.0 218.142.21.231 255.255.255.255

2.3. 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: 10.132.6.96
- Nom del domini Local: 10.132.6.96

2.4. Interfícies

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	Alias	Address/FQDN	DHCPRelay
port1	Outside	10.132.0.254 255.255.255.0	-
port2	Inside-srv	10.132.6.254 255.255.255.0	-
port3	Inside-wrk	10.132.4.254 255.255.255.0	10.132.6.96
port4	Outside-wlan	10.132.7.254 255.255.255.0	-

2.5. Taula d' enrutament

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	Interficie	Prioritat
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 a través de les interfícies wan per detectar la caiguda de les línies de comunicacions.

Servidor desti	GW	Interficie	Interval	Failtime	Recovery
8.8.4.4	10.132.0.1	port1	3	3	3
8.8.4.4	10.132.7.1	port4	3	3	3

2.6. Objectes Adreces del Firewall

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

Name	Category	Address/FQDN	Interface	Type*
inside_srv	Address	10.132.6.0	Any	Subnet
inside_wrk	Address	10.132.4.0	Any	Subnet
cloud1	Address	5.125.205.142	Any	Subnet
cloud2	Address	91.117.121.65	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)

2.7. Objectes Serveis

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	Categoria	Ports TCP	Ports UDP	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	-	-
HTTPS	Web Access	443	-	-
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	-	119	-	-

Nom del servei	Categoria	Ports TCP	Ports UDP	Protocol
NTP	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	-	514:512-1023	-	-
SCCP	VoIP, Messaging & Other Applications	2000	-	-
SIP	VoIP, Messaging & Other Applications	5060	5060	-
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	-	-

Nom del servei	Categoria	Ports TCP	Ports UDP	Protocol
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	Categoria	Ports TCP	Ports UDP	Protocol
8083_TCP	-	8083	-	-
43421_UDP	-	0	43421	-

2.8. NATs d'entrada (Virtual IPs)

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

Name	External IP Address/Range	External Service Port	Mapped IP Address/Range	Map to Port
VIP_srv-01	port1/10.132.0.254	43421/udp	10.132.6.62	-
VIP-srv-02	port1/10.132.0.254	8083/tcp	10.132.6.97	8083/tcp

2.9. Polítiques de Firewall

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

ID	From	To	Source	Destinatio	Service	Action	AV	Web Filter	App Control	IPS	SSL INSPECT	LOG	NAT
1	port3/inside_wrk	port4	inside_wrk(-)	all	ALL	accept	UTM-AV	UTM-WF	UTM-APP	UTM-IPS	-	all	enable
2	port3/inside_wrk	port2	inside_wrk(-)	inside_srv	ALL	accept	-	-	-	-	-	disable	-
3	port2/inside_srv	port3	inside_srv(-)	inside_wrk	ALL	accept	-	-	-	-	-	disable	-
4	port3/inside_wrk	port1	inside_wrk(-)	all	ALL	accept	UTM-AV	UTM-WF	UTM-APP	UTM-IPS	-	all	enable
5	port2/inside_srv	port1	inside_srv(-)	all	ALL	accept	UTM-AV	UTM-WF	UTM-APP	UTM-IPS	-	all	enable
6	port2/inside_srv	port4	inside_srv(-)	all	ALL	accept	UTM-AV	UTM-WF	UTM-APP	UTM-IPS	-	all	enable
7	ssl.root/vpn-net	port2	vpn-net(Global)	inside_srv	ALL	accept	-	-	-	-	-	all	enable
8	ssl.root/vpn-net	port3	vpn-net(Global)	inside_wrk	ALL	accept	-	-	-	-	-	all	enable
9	port1/cloud1 cloud2	port2	cloud1 cloud2(-)	VIP-srv-01	8083_TCP	accept	-	-	-	-	-	all	-
	Any	Any	ALL	ALL	ALL	DENY							

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 te com el perfil d'antivirus activat UTM-AV que detecta i neteja malware i possibles connexions a xarxes de Botnets.

2.11. Servei de Filtratge Web

El servei de filtratge de web, proveeix d'un servei de filtratge de contingut web a través dels pprotocols 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 activa 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 client, de criticitat "critical" i "high" que afectin a serveis
de sistemes operatius Windows, Linux i MacOS.