

Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	

Objectif

Cette note technique a pour objectif de fournir le paramétrage requis pour la mise en place un portail captif grâce à la distribution zeroshell

Principe de fonctionnement

La distribution zeroshell va permettre de faire le lien entre l'interface lan et wan en filtrant les connexions grâce au portail captif.

Les connexions au portail captif vont se faire grâce au protocole kerberos 5 qui va permettre l'authentification des comptes du domaine installé sur un serveur windows 2012 r2.

Prérequis

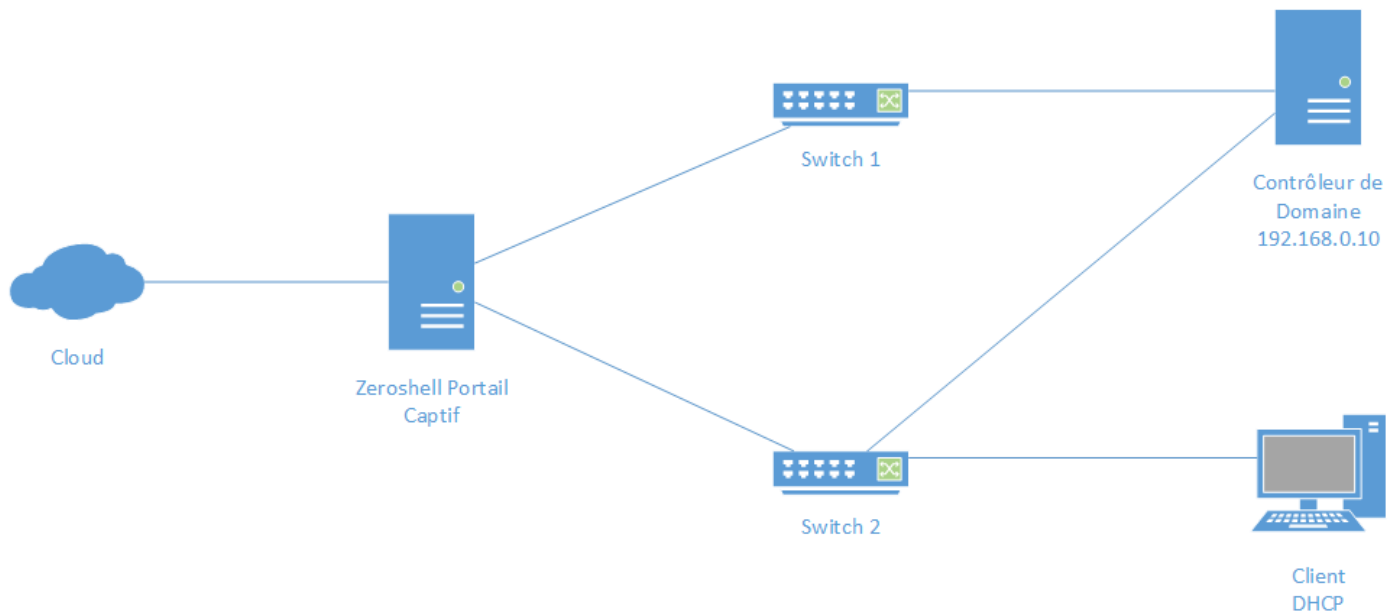
Créer les vm suivantes :

- Zeroshell dont l'installation est décrit ci-dessous
- Une machine cliente sous Windows 7
- Un serveur Windows 2012 r2 avec le rôle AD-ADS (domaine active directory) installé

Configuration du serveur Windows

- **Configuration élémentaire du serveur Windows 2012 r2**
 - Renommer le serveur : `Rename-Computer -NewName "nom" (shutdown /R)`
 - Autoriser le ping du serveur dans le pare-feu : `netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol="icmpv4:8,any" dir=in action=allow`
 - Configurer windows update sur rechercher les maj mais ne pas les installés avec sconfig
 - Configurer le bureau à distance avec sconfig

Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	



Architecture NIC Teaming avec Windows Server 2012 r2 et Zeroshell

- **Configurer les interfaces réseau en mode association de carte réseau pour permettre la haute disponibilité et la tolérance aux pannes**
 - Créer une nouvelle équipe de carte réseau
 - Sélectionner les deux cartes réseau
 - Mode d'équipe sur indépendant du commutateur : liaison sur deux switch
 - Hachage d'adresse : utilise les adresses MAC, les adresses IP et les ports TCP

Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	

Association de cartes réseau

Nouvelle équipe

Nom de l'équipe :
Zeroshell

Cartes membres :

Dans l'équipe	Carte	Vitesse	État	Raison
<input checked="" type="checkbox"/>	Ethernet0	1 Gbits/s		
<input checked="" type="checkbox"/>	Ethernet1	1 Gbits/s		

Propriétés supplémentaires

Mode d'équipe : Indépendant du commutateur

Mode d'équilibrage de charge : Hachage d'adresse

Carte réseau en attente : Aucun (toutes les cartes actives)

Interface d'équipe principale : [Zeroshell - VLAN par défaut](#)

OK Annuler

- Configuration finale de l'association des cartes réseau

Association de cartes réseau

SERVEURS
Tous les serveurs | 1 au total

Nom	Statut	Type de serveur	Version du système d'exploitation	Équipes
SERV-01	En ligne	Physique	Microsoft Windows Server 2012 R2 Standard	1

ÉQUIPES
Toutes les équipes | 1 au total

Équipe	Statut	Mode d'équipe	Équilibrage de charge	Cartes
Zeroshell	OK	Indépendant du commutateur	Hachage d'adresse	2

CARTES ET INTERFACES

Carte	Vitesse	État	Raison
Zeroshell (2)			
Ethernet0	1 Gbits/s	Actif	
Ethernet1	1 Gbits/s	Actif	

Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	

● Configuration finale du serveur

PROPRIÉTÉS Pour serv-01		TÂCHES ▼	
Nom de l'ordinateur	serv-01	Dernières mises à jour installées	Jamais
Domaine	dom-test.local	Windows Update	Rechercher les mises à jour uniquement à l'aide de Windows Update
		Dernière recherche de mises à jour :	Jamais
Pare-feu Windows	Domaine : Actif	Rapport d'erreurs Windows	Inactif
Gestion à distance	Activé	Programme d'amélioration de l'expérience utilisateur	Non participant
Bureau à distance	Activé	Configuration de sécurité renforcée d'Internet Explorer	Actif
Association de cartes réseau	Activé	Fuseau horaire	(UTC+11:00) Îles Salomon, Nouvelle-Calédonie
Zeroshell	192.168.0.10, Compatible IPv6	ID de produit (Product ID)	Non activé
Version du système d'exploitation	Microsoft Windows Server 2012 R2 Standard	Processeurs	Intel(R) Core(TM) i7-5700HQ CPU @ 2.70GHz
Informations sur le matériel	VMware, Inc. VMware Virtual Platform	Mémoire installée (RAM)	2 Go
		Espace disque total	60 Go

● Installation du contrôleur de domaine

- Installation des rôles ADDS ainsi que des RSAT avec la console powershell
 - Get-WindowsFeature
 - Add-WindowsFeature AD-Domain-Services -IncludeAllSubFeature -Restart
 - Add-WindowsFeature RSAT-AD-Tools -IncludeAllSubFeature -Restart
- Création du domaine avec un script powershell

#

Script Windows PowerShell pour le déploiement d'AD DS

#

Import-Module ADDSDeployment

Install-ADDSForest `

-CreateDnsDelegation:\$false `

-DatabasePath "C:\Windows\NTDS" `

-DomainMode "Win2012R2" `

-DomainName "dom-test.local" `

-DomainNetbiosName "DOMTEST" `

-ForestMode "Win2012R2" `

-InstallDns:\$true `

-LogPath "C:\Windows\NTDS" `

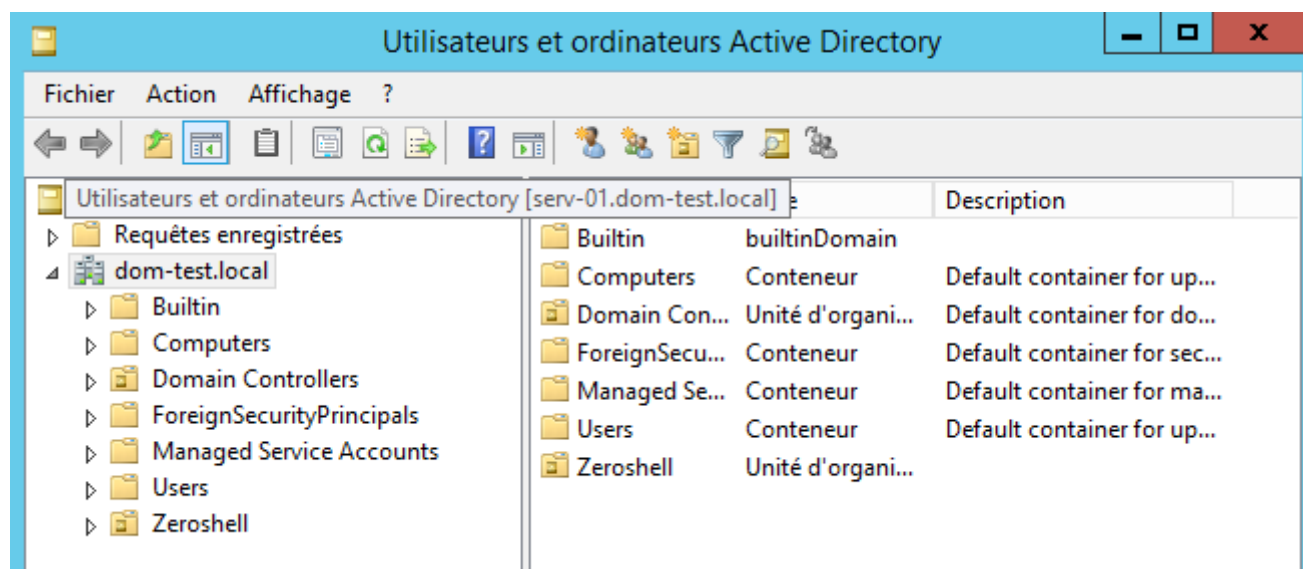
-NoRebootOnCompletion:\$false `

Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	

-SysvolPath "C:\Windows\SYSVOL" `

-Force:\$true

- **Arborescence du domaine dom-test.local**



Configuration IP des machines

	Adresse IP	Passerelle	Serveur DNS
Windows 7	DHCP	192.168.0.75 Zeroshell	192.168.0.10 Win 2012 r2
Win 2012 Server	192.168.0.10/24	192.168.0.75 Zeroshell	192.168.0.10 Win 2012 r2
Zeroshell	ETH00 : 192.168.0.75/24 ETH01 : 192.168.75.75/24		

Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	

Configuration du serveur Zeroshell

- Configurer les interfaces Ip du Wan et du Lan à l'aide du shell
 - Ip Wan : 192.168.75.75
 - Ip LAN : 192.168.0.75

```

-----
ETH00 - Advanced Micro Devices, Inc. [AMD] 79c970 [PCnet32 LANCE] (rev 10)
Status: Duplex
(1) 192.168.75.75 / 255.255.255.0 (up)
-----
ETH01 - Advanced Micro Devices, Inc. [AMD] 79c970 [PCnet32 LANCE] (rev 10)
Status: Duplex
-----
Default Gateway: none

COMMANDS
<A> Add IP address          <D> Delete IP address
<M> Modify IP address       <G> Set Default Gateway
<S> Change Interface status <H> Dynamic IP configuration
<I> Show Info               <Q> Quit
>> _

```

- Pour que Zeroshell sauvegarde les paramètres des profils il faut créer une partition et les enregistrer :
 - Création de partition sda1 de type ext4 dans /Setup/Profiles

ATA VMware Virtual I (sda)

[Refresh](#) [Close](#)

Disk /dev/sda: 8589 MB, 8589934592 bytes
 255 heads, 63 sectors/track, 1044 cylinders, total 16777216 sectors
 Units = sectors of 1 * 512 = 512 bytes
 Sector size (logical/physical): 512 bytes / 512 bytes
 I/O size (minimum/optimal): 512 bytes / 512 bytes

Partition Size

- ☐ Fixed Size GB
☒ Max Available

Label

Filesystem type

- ☒ Format now
☒ Extended 4 (journalized)
☐ Extended 3 (journalized)
☐ Reiserfs (journalized)
☐ Extended 2 (unjournalized)

Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	

- Création du profil sur la partition créée :

ATA VMware Virtual I (sda)

New Profile on partition sda1

Create Close

Description	Tp zeroshell		
Hostname (FQDN)	zeroshell.local		
Kerberos 5 Realm	ZEROSHELL.LOCAL		
LDAP Base	dc=zeroshell,dc=local		
Admin password	****		
Confirm password	****		
NETWORK CONFIG			
Ethernet Interface	ETH00 - Advanced Micro Devices, Inc. [AMD] 79c970 [PCnet32 LANCE] v		
IP Address / Netmask	192.168.75.75	/	255.255.255.0
Default Gateway	192.168.75.2		

- Restriction d'accès au serveur zeroshell :
 - Restriction d'accès à l'interface d'administration web aux postes du réseau local :

HTTPS Web Interface Settings

Save Close

HTTP Port HTTPS Port **Note:** port changes take effect at the next boot time

Allow access from ☐ Auto-authorize LAN IP Interface + -

Subnet 10.0.0.0/8
Subnet 172.16.0.0/12
Subnet 192.168.0.0/16

- Restriction d'accès en SSH aux postes du réseau local :

Secure Shell Settings

☐ Enabled Save Close

Allow access only from IP Interface + -

Subnet 192.168.0.0/24

Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	

Configuration du portail captif

- Configuration du NAT pour permettre la communication entre l'interface WAN et LAN
 - Sélection de l'interface ETH00 : interface WAN

Network Address Translation Save View Close

Available Interfaces

ETH01
 ETH02
 VPN99

>>>
 <<<

NAT Enabled Interfaces

ETH00

Note:
the source IP of outgoing packets from the enabled NAT interfaces will be automatic translated using routing table (MASQUERADE)

- Sélection de l'interface ou le portail captif sera actif :

MULTI Interface Configuration Ok Close

Available Interfaces

ETH00
 VPN99

>>>
 <<<

MULTI Interface

ETH01

Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	

- Configuration du portail captif
 - Configurer Auth Validity sur 1 min pour restreindre l'accès au portail après avoir fermé la fenêtre d'authentification

Gateway Parameters	
DoS Protection	Medium ▾
Client Identity	IP and MAC address ▾
Simultaneous Connections	Allowed ▾
Authenticator Validity	5 ▾ minutes Popup

- Configurer les machine qui n'auront pas besoin de s'authentifier sur le portail à savoir le windows serveur
 - Ajouter l'Ip et l'adresse Mac du poste

Free Authorized Client Save Close

Description	Windows serveur
IP Address	192.168.0.10
MAC Address	00:0C:29:70:C5:BF

- Le poste autoriser apparaît dans l'onglet free authorized puis dans la sous-catégorie client :

Free Authorized Clients ▾ + -		
Description	IP Address	MAC Address
⦿ Fabien	192.168.0.30	AA:BB:CC:DD:EE:FF

Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	

- Pour permettre l'authentification des client avec l'Active directory il faut configurer l'authentification kerberos externe
 - Pour cela se rendre dans l'onglet Security puis sur Kerberos Realms
 - Ensuite il faut ajouter une entrée
 - Le nom du domaine dans Realm : dom-test.local
 - Puis l'ip du serveur dans KDC

Kerberos 5 Realms

Close

Realm KDC Add

Key Distribution Center List

Remove

ZEROSHELL.LOCAL (KDC: Local)
DOM-TEST.LOCAL (KDC: 192.168.0.10)

Use the DNS to discovery Realms and KDC servers not configured

No

- Ensuite il faut configurer le domaine comme autorisé pour l'authentification du portail captif :

Authorized Domain

Save Close

Domain Name

Domain Type

- ☐ Local Kerberos 5 Realm
☒ External Kerberos 5 Realm
☐ Trusted Kerberos 5 Realm (*)
☐ RADIUS Proxy Domain (**)

Radius Request

Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	

- Il suffit pour vérifier le fonctionnement de se connecter avec un poste client



Captive Portal Web Login

Network Access Example

Otranto (Lecce) - Italy

AAI

Cert

Username

Password

Domain

dom-test.local ▼

Network Access

[Info](#)

Powered by ZeroShell - Net Services

- La connexion a été acceptée

Network Access

Redirect

Fabien@dom-test.local successfully authenticated

Connecting to the Network...

Powered by ZeroShell - Net Services


Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	

- Pour garantir la connexion il ne faut pas quitter cette fenêtre de connexion


Network Access
Disconnect

Fabien@dom-test.local connected - IP:192.168.0.2

Time	:	0:00	Refresh
Traffic	:	0.00 MB	
Cost	:	0.00 €	


Powered by ZeroShell - Net Services

- Ainsi dans l'onglet portail captif le client connecté apparaît

Connected Clients: 1			Disconnect	Refresh
	Username	IP Address	MAC Address	
	Fabien@dom-test.local	192.168.0.2	00:0c:29:e7:e7:f7	

Mise en place du serveur DHCP

- Mise en place du service DHCP sur l'interface LAN avec comme réseau 192.168.0.0/24

New DHCP Subnet definition

Available	192.168.0.0/255.255.255.0 (ETH01) ▼
Network	192.168.0.0
Netmask	255.255.255.0

OK Cancel

- Création du pool d'adresse pour l'interface LAN
 - Paramétrage du bail DHCP entre 8 et 12h
 - Pool : 192.168.0.1 : 192.168.0.74
 - Ip de l'interface zeroshell 192.168.0.75

Dynamic IP Configuration

	Default Lease Time				Max Lease Time		
	Days	Hours	Minutes		Days	Hours	Minutes
	00 ▼	08 ▼	00 ▼		00 ▼	12 ▼	00 ▼
Range 1	192.168.0.1			-	192.168.0.74		
Range 2				-			
Range 3				-			

- Parametragage des options du DHCP
 - Passerelle par défaut
 - DNS du Windows serveur 192.168.0.10

Subnet Options

Advanced

Default Gateway	192.168.0.75
DNS 1	8.8.8.8
DNS 2	
DNS 3	
Domain Name	
NIS Domain	
NTP Server	
WINS Server	

Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	

- Réservation d'une adresse IP pour le serveur Windows :

DHCP STATIC ENTRY		192.168.0.0/255.255.255.0
Description	<input type="text" value="Windows serveur"/>	
Fixed IP	<input type="text" value="192.168.0.10"/>	
MAC Address	<input type="text" value="00:0C:29:70:C5:BF"/>	

- Analyse des log d'une requête DHCP par un client (192.168.0.2)
 - DHCPDISCOVER : Diffusion d'une trame en Broadcast (port 67)
 - DHCPOFFER : Réponse des serveurs DHCP (port 68)
 - DHCPREQUEST : Demande de l'adresse ip au serveur DHCP (unicast)
 - DHCPACK : Confirmation du serveur DHCP

```

20:40:10 DHCPDISCOVER from 00:0c:29:e7:e7:f7 via ETH01
20:40:10 DHCPOFFER on 192.168.0.2 to 00:0c:29:e7:e7:f7 (Fabien1-PC) via ETH01
20:40:10 DHCPREQUEST for 192.168.0.2 (192.168.0.75) from 00:0c:29:e7:e7:f7 (Fabien1-PC) via ETH01
20:40:10 DHCPACK on 192.168.0.2 to 00:0c:29:e7:e7:f7 (Fabien1-PC) via ETH01
20:40:14 DHCPINFORM from 192.168.0.2 via ETH01
20:40:14 DHCPACK to 192.168.0.2 (00:0c:29:e7:e7:f7) via ETH01

```

Mise en place de la monétisation du portail captif

- Mise en place d'un système de monétisation :
 - Paieement après utilisation de la connexion : post paiement
 - Paramétrage du coût par megabyte à 5€
 - Restriction du temps de connexion à 5h
 - Limitation de la bande passante à 100 Mbit/s

Accounting Class

Save Close

Class Name

BILLING

Type of Charge

Postpaid ▾

Cost per Megabyte (€)

5

Cost per Hour (€)

Time and Traffic Limits take effect if specified

LIMITS

Traffic (MBytes)

Time (Hours)

5

Bandwidth (Mbit/s)

100

- Association d'un compte créé sur zeroshell

RADIUS Accounting

Expiration (mm/dd/yyyy)

▾

▾

▾

Accounting Class

POSTPAIEMENT ▾

Credit: 0.00 €

+

-

^

▾

Limits

- MB

5 h

100 Mb/s

Costs (postpaid)

5.00€/MB

0.00€/h

- Visualisation du paiement en temps réel via la fenêtre de connexion

Network Access

Disconnect

Fabien@DOM-TEST.LOCAL connected - IP:192.168.0.2

Time	:	0:01	Refresh
Traffic	:	9.54 MB	
Cost	:	44.58 €	

Powered by ZeroShell - Net Services

Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	

Mise en place de l'un proxy http

- Mise en place du proxy transparent sur l'interface LAN : 192.168.0.0/24

Proxy Capturing Rule		Save Close
Action	Capture Request	
Source Interface/VLAN	ETH01	
Source IP (*)	192.168.0.0/24	
Destination IP (*)		

- Mise en place des règles
 - Activation de l'antivirus
 - Mise en place d'une blacklist pour les site en http

HAVP Configuration	
Access Logging (check the law in your country)	Any Access
ClamAV Antivirus Configuration	
Virus Scanning	Enabled
Check Images (jpg, gif, png)	Enabled
AutoUpdate Virus Signatures	Enabled
Number of Checks per Day	12
Country of the Mirror	New Caledonia
URL Management	
Blacklist (1 items)	Manage Enabled
Whitelist (0 items)	Manage Disabled

- Analyse des logs
 - Requete du poste 192.168.0.2


```
21:26:02 192.168.0.2 GET 204 http://www.gstatic.com/generate_204 105+0 OK
21:26:21 192.168.0.2 GET 204 http://www.gstatic.com/generate_204 105+0 OK
21:26:29 192.168.0.2 GET 0 http://www.google.fr/ 0+0 BLACKLIST
21:26:30 192.168.0.2 GET 200 http://www.google.fr/favicon.ico 415+1494 OK
```


Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	

Mise en place de la qualité de service (QoS)

- Mise en place des classes pour différencier les types de données :

QoS - CLASS MANAGER

Save New Delete Close

VOIP Description VOIP
Priority High DSCP Maximum 16 Mbit/s Guaranteed 16 Mbit/s

Class	Description	Priority	DSCP	Max Bandwidth	Guaranteed On
<input type="radio"/> DEFAULT	Default class for unclassified traffic	Medium			<input checked="" type="checkbox"/>
<input type="radio"/> P2P	Limite le P2P	Low		16Mbit/s	1Kbit/s <input checked="" type="checkbox"/>
<input type="radio"/> SHELL	SSH	High		16Mbit/s	16Mbit/s <input checked="" type="checkbox"/>
<input checked="" type="radio"/> VOIP	VOIP	High		16Mbit/s	16Mbit/s <input checked="" type="checkbox"/>

- Création des règles pour chaque classe :
 - Filtrage par port : 443 port HTTPS
 - Interface source et destination du trafic
 - Adresse ip source : 192.168.0.0/24
 - Puis dans target class associer la règle a la bonne classe puis activer la journalisation

QoS Apply to Routed and Bridged Packets Sequence 2 + - Confirm Close

Description Navigation Web HTTPS

Packet Matching	Description	Value	Not								
	Input	ETH02	<input type="checkbox"/>								
	Output	ETH00	<input type="checkbox"/>								
	Source IP (*)	192.168.0.0/24	<input type="checkbox"/>								
	Destination IP		<input type="checkbox"/>								
	Fragments	[<input type="checkbox"/> match only second and further fragments]	<input type="checkbox"/>								
	Packet Length	-	<input type="checkbox"/>								
Source MAC		<input type="checkbox"/>									
Protocol Matching <input type="checkbox"/> Not	Source Port <input type="checkbox"/> Not	Dest. Port <input type="checkbox"/> Not	Opt <input type="checkbox"/> Not	Flags <input type="checkbox"/> Not	SYN <input type="checkbox"/> Not	ACK <input type="checkbox"/> Not	FIN <input type="checkbox"/> Not	RST <input type="checkbox"/> Not	URG <input type="checkbox"/> Not	PSH <input type="checkbox"/> Not	
TCP	443										
Connection State <input type="checkbox"/> Not	<input checked="" type="checkbox"/> NEW <input checked="" type="checkbox"/> ESTABLISHED <input type="checkbox"/> RELATED <input type="checkbox"/> INVALID <input type="checkbox"/> UNTRACKED										
IPTABLES Parameters <input type="button" value="Manual"/>											
Time Matching	From : to : <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun										
nDPI Deep Packet Inspection	Matching <input type="checkbox"/> Not <input type="button" value="nDPI Manager"/>										
Layer 7 Filters	Protocol Description <input type="checkbox"/> Not <input type="button" value="L7 Manager"/>										
DiffServ	DSCP										
Connection Limits	Parallel connections per IP more than Traffic per connection more than MB										
TARGET CLASS DEFAULT <input checked="" type="checkbox"/> LOG 10 / Day Burst 15											

Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	

- Visualisation des règles dans l'onglet classifier :
 - Deux règles sont présente :
 - HTTP et HTTPS

Chain: QoS		Policy None		Chain QoS	New	Remove	View	Show Log
Save		Cancel		Enabled <input checked="" type="checkbox"/>				
QoS Rules				Add Change Delete				
	Seq	Input	Output	Description	QoS Class	Log	Active	
<input type="radio"/>	1	ETH02	ETH00	MARK tcp opt -- in ETH02 out ETH00 192.168.0.0/24 -> 0.0.0.0/0 state NEW,ESTABLISHED tcp spt:80 /* Navigation web */ MARK set 0xa	DEFAULT	yes	<input checked="" type="checkbox"/>	
<input checked="" type="radio"/>	2	ETH02	ETH00	MARK tcp opt -- in ETH02 out ETH00 192.168.0.0/24 -> 0.0.0.0/0 state NEW,ESTABLISHED tcp spt:443 /* Navigation Web HTTPS */ MARK set 0xa	DEFAULT	yes	<input checked="" type="checkbox"/>	

- Association des classes a l'interface lan à savoir ETH02

ETH02 1000Mb/s Full Duplex							On <input checked="" type="checkbox"/>
Intel Corporation 82545EM Gigabit Ethernet Controller (Copper) (rev 01)							<input checked="" type="checkbox"/>
QoS Status:Enabled Max:1000Mbit/s Guaranteed:1000Mbit/s (Assigned:3%)							
	Class	Description	Priority	DSCP	Max Bandwidth	Guaranteed	On
<input type="radio"/>	DEFAULT	Default class for unclassified traffic	Medium				<input checked="" type="checkbox"/>
<input type="radio"/>	P2P	Limite le P2P	Low		16Mbit/s	1Mbit/s	<input checked="" type="checkbox"/>
<input type="radio"/>	SHELL	SSH	High		16Mbit/s	16Mbit/s	<input checked="" type="checkbox"/>
<input type="radio"/>	VOIP	VOIP	High		16Mbit/s	16Mbit/s	<input checked="" type="checkbox"/>

- Visualisation des statistiques de données envoyé en bytes par classes

QoS STATISTICS			Interface ALL	Graphics	Refresh	Close
Interface/Class	Priority	DSCP	Maximum	Guaranteed	Traffic Sent (bytes)	Rate
ETH02	--	--	1000Mbit/s	1000Mbit/s	175844	63440bit
DEFAULT	Medium		16Mbit/s	10Mbit/s	175844	63440bit
P2P	Low		16Mbit/s	1Mbit/s	0	0bit
SHELL	High		16Mbit/s	16Mbit/s	0	0bit
VOIP	High		16Mbit/s	16Mbit/s	0	0bit

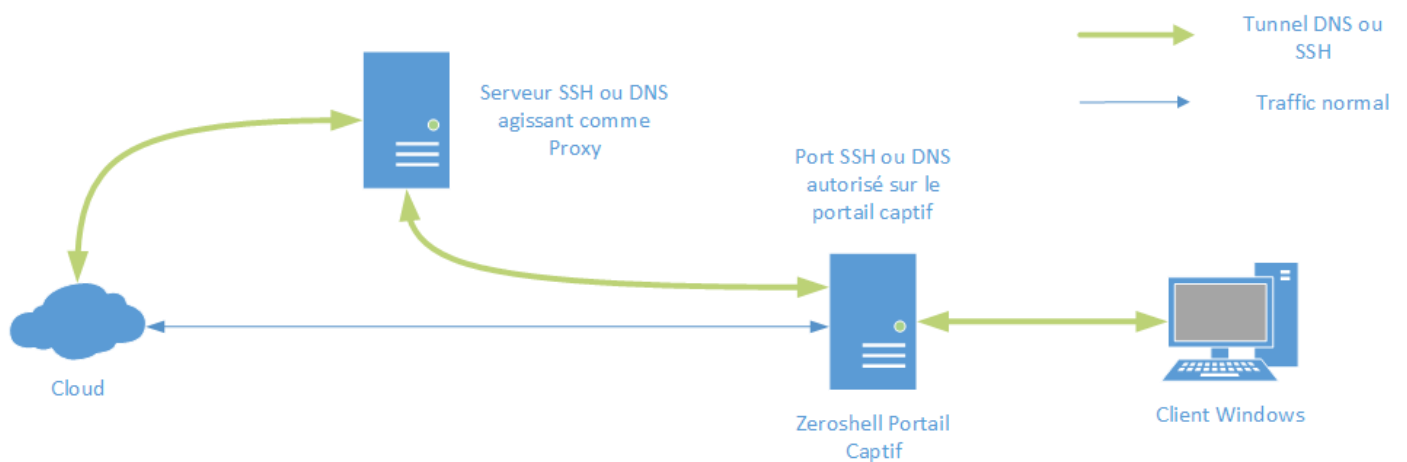
Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	

Etude d'une attaque pour contourner le portail captif

- Architecture de l'attaque



Utilisation normal du portail captif



Attaque par SSH ou DNS Tunneling

Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	

- Mise en place de l'attaque
 - Configuration des ports autorisé par défaut par le portail captif sans avoir besoin de s'authentifier

Free Authorized Services ▼			+	-
Description	IP Address	Port		
<input type="radio"/> Domain Name System	Any	53/udp		
<input type="radio"/> DHCP and bootp	Any	67/udp		
<input type="radio"/> SSH	Any	22/tcp		

- Avoir au préalable un serveur SSH ou DNS configuré avec le port forwarding d'activé
- Vérification de l'autorisation du port ssh sur le client windows avec nmap

■ Port bloqué

```
nmap -p 22 192.168.75.165
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-03 23:17 Pacifique Centre
Nmap scan report for 192.168.75.165
Host is up (0.00013s latency).
PORT      STATE      SERVICE
22/tcp    filtered  ssh
Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
```

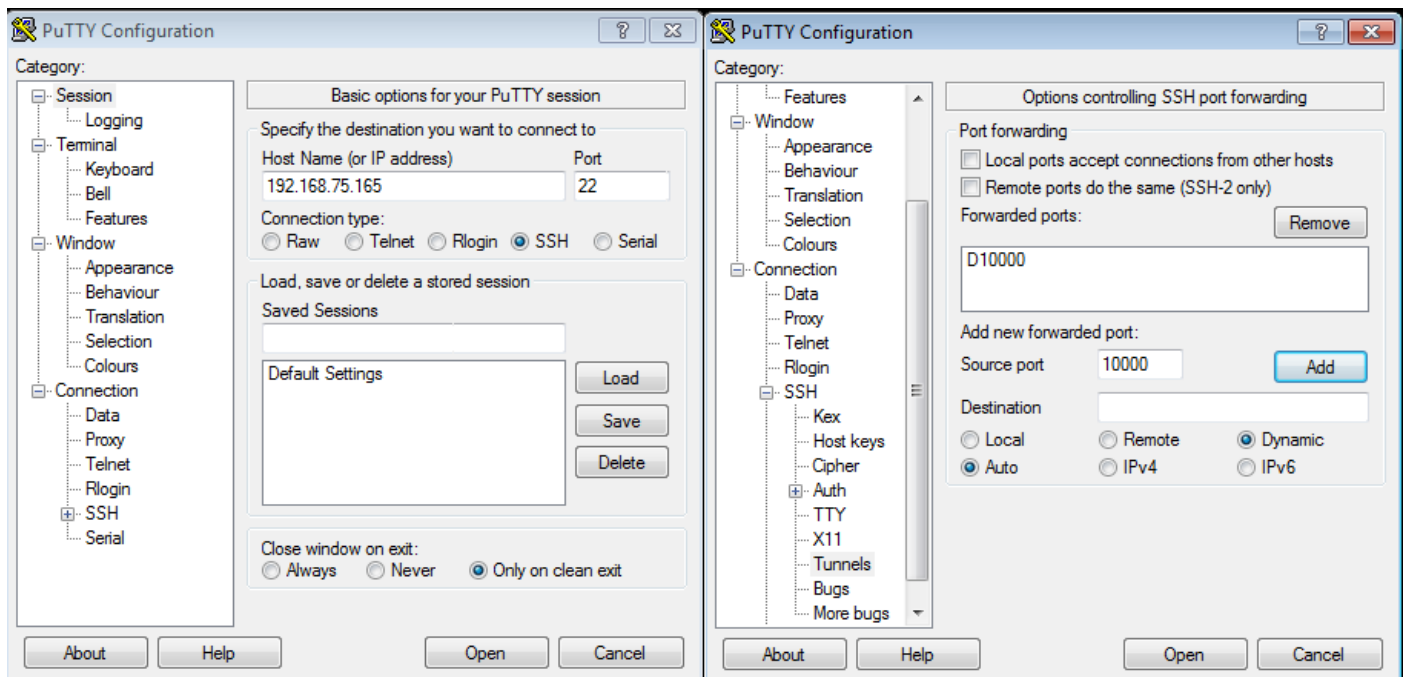
■ Port autorisé

```
nmap -p 22 192.168.75.165
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-03 23:18 Pacifique Centre
Nmap scan report for 192.168.75.165
Host is up (0.0011s latency).
PORT      STATE      SERVICE
22/tcp    open      ssh
Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
```

Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	

- Création du tunnel ssh avec putty en accédant au serveur configuré au préalable
 - Ip du serveur : 192.168.75.165
 - Configuration du port forwarding : mapper le port 10000 en local



- Configuration du proxy socks dans le navigateur mozilla

☒ Configuration manuelle du proxy :

Proxy HTTp : Port :

☐ Utiliser ce serveur proxy pour tous les protocoles

Proxy SSL : Port :

Proxy FTP : Port :

Hôte SOCKS : Port :

☐ SOCKS v4 ☒ SOCKS v5

Fabien Mauhourat	Note Technique	Révision : 01 Edition : 24/04/2017
	Mise en place d'un portail captif	

o Vérification de la connexion avec une analyse de trame

1	0.000000	192.168.75.165	192.168.0.2	SSH	134 Server: Encrypted packet (len=80)
2	0.000218	192.168.0.2	192.168.75.165	SSH	102 Client: Encrypted packet (len=48)
3	0.000345	192.168.75.165	192.168.0.2	TCP	60 22→1124 [ACK] Seq=81 Ack=49 Win=1025 Len=0
4	1.786988	192.168.0.2	192.168.0.75	DNS	76 Standard query 0x0afc A www.facebook.com
5	1.821422	192.168.0.75	192.168.0.2	DNS	244 Standard query response 0x0afc A www.facebook.com CNAME
6	1.822298	192.168.0.2	192.168.0.75	DNS	87 Standard query 0xc7df A star-mini.c10r.facebook.com
7	1.822437	192.168.0.75	192.168.0.2	DNS	226 Standard query response 0xc7df A star-mini.c10r.facebook.com
8	1.823130	192.168.0.2	192.168.75.165	SSH	166 Client: Encrypted packet (len=112)
9	1.823346	192.168.75.165	192.168.0.2	TCP	60 22→1124 [ACK] Seq=81 Ack=161 Win=1024 Len=0
10	1.823883	192.168.0.2	192.168.0.75	DNS	87 Standard query 0x8930 AAAA star-mini.c10r.facebook.com
11	1.858166	192.168.0.75	192.168.0.2	DNS	238 Standard query response 0x8930 AAAA star-mini.c10r.facebook.com
12	2.045899	192.168.75.165	192.168.0.2	SSH	118 Server: Encrypted packet (len=64)
13	2.046137	192.168.0.2	192.168.75.165	SSH	310 Client: Encrypted packet (len=256)
14	2.046293	192.168.75.165	192.168.0.2	TCP	60 22→1124 [ACK] Seq=145 Ack=417 Win=1022 Len=0
15	2.275155	192.168.75.165	192.168.0.2	SSH	1478 Server: Encrypted packet (len=1424)
16	2.277245	192.168.75.165	192.168.0.2	SSH	1478 Server: Encrypted packet (len=1424)
17	2.277338	192.168.0.2	192.168.75.165	TCP	54 1124→22 [ACK] Seq=417 Ack=2993 Win=16425 Len=0