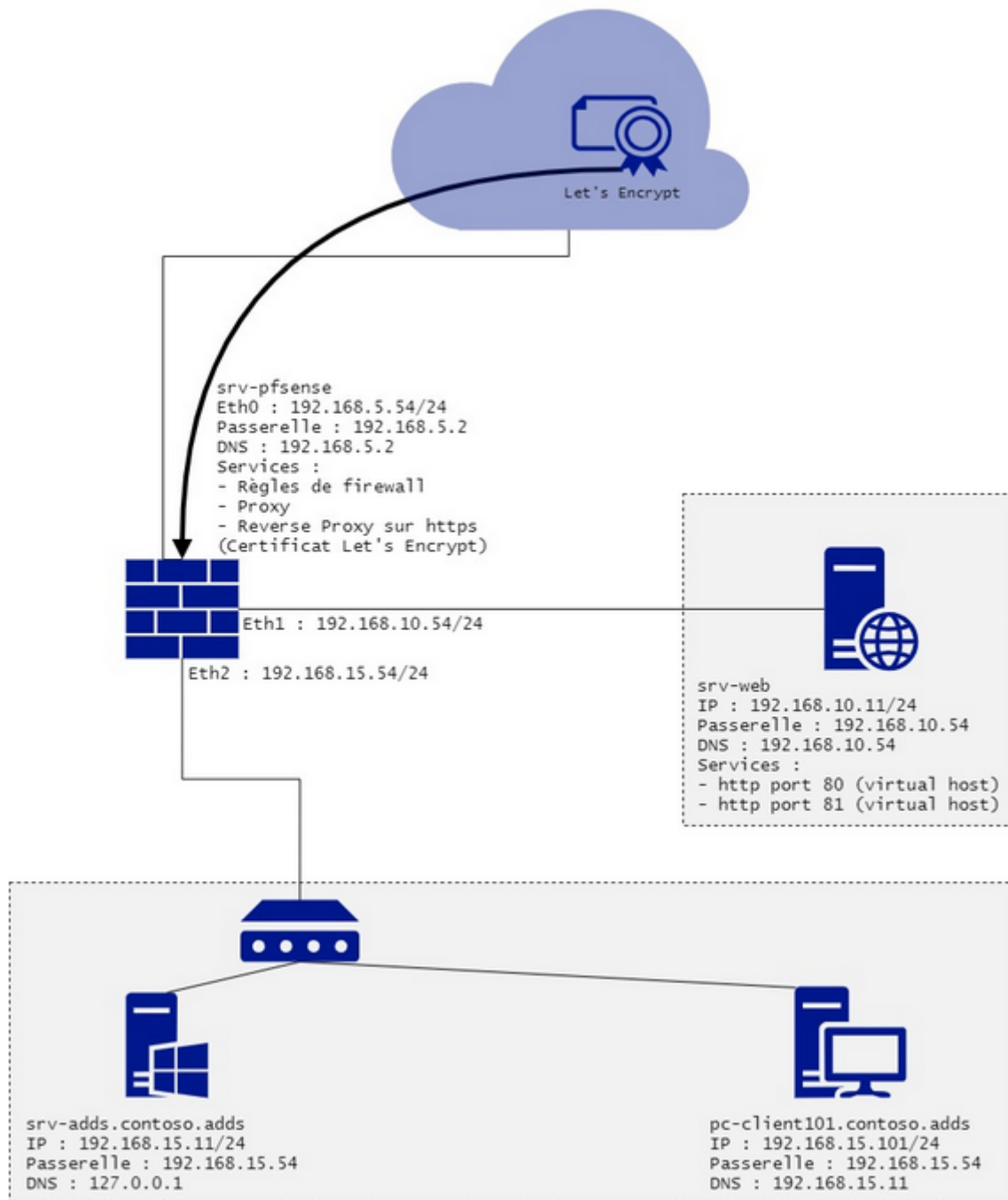


Année 2020 - 2021

L'objectif de ce dossier technique est de mettre en place une architecture similaire à celle-là :

Schéma de l'infrastructure

Fabien LAFAGE



DOSSIER TECHNIQUE

Durée :

32h

Introduction :

Sécurité des systèmes d'informations (Linux/Windows)
Établir les bases nécessaires à la compréhension de la problématique (concepts, terminologie, classification)
Dresser un panorama global des risques et des solutions
Illustrer ces concepts et solutions par des réalisations pratiques
Les positionner dans le contexte du monde actuel via des études de cas
Comprendre ce qu'est la PRA (Plan de Reprise d'Activité) et la redondance pour la continuité des services

Solutions à mettre en œuvre :

Le firewall devra remplir les rôles de : Gestion des flux, Proxy, Reverse Proxy, Détection d'intrusion
Le contrôleur de domaine devra permettre la gestion du DNS local et des GPO qui seront appliquées au poste client
La gestion des flux entrants et sortants devra être gérée par le firewall, seuls les ports 80 et 443 seront autorisés
Le Proxy lié au service SquidGuard, devra permettre la gestion du blocage de noms de domaines / url etc en sortie
Le Reverse Proxy devra permettre l'accès au travers d'un nom de domaine unique et de ses 2 sous-domaines à 2 Virtual Host (ports 80 et 81) hébergés sur le serveur Web, le tout devra être chiffré sur le protocole https côté WAN du firewall
La configuration du Proxy sera poussée sur les navigateurs Edge et Firefox des postes clients par GPO

Mise en place d'une infrastructure comprenant :

- 1 firewall
- 1 serveur Web
- 1 contrôleur de domaine
- 1 client

Installation + configuration de l'ISO pfSense

Create a new VM → Custom → workstation 16.x

I will install the operatin system later pour empêcher la creation de fichiers de reponses automatiques

FreeBSD 12-64 bits → version

Nb process → 1

Nb core → 2 / 4

Memory of this virtual machine → 512 MB

Network type → NAT

Disk → 40G → store virtual disk as a single file

On ajoute 2 nouvelles cartes réseaux secu-DMZ / secu-LAN

On fait une snapshot

On ajoute l'iso pfsense au CV/DVD puis on exec

On accepte, choix langue, choix BIOS puis on installe

On config l'IP du WAN sur 192.168.5.54 sur la passerelle 192.168

On configure la 3^e carte réseau non reconnu (em2) en tant que LAN

```
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y!n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 a or nothing if finished): em2

Enter the Optional 1 interface name or 'a' for auto-detection
(em1 a or nothing if finished): em1

The interfaces will be assigned as follows:

WAN   -> em0
LAN   -> em2
OPT1  -> em1

Do you want to proceed [y!n]? █
```

On définit le LAN sur l'adresse 192.168.15.54

On démarre une VM Client que l'on met sur le segment secu-LAN

On modifie l'adresse IP :

Propriétés de : Protocole Internet version 4 (TCP/IPv4) X

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 192 . 168 . 15 . 101

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : 192 . 168 . 15 . 54

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 192 . 168 . 15 . 54

Serveur DNS auxiliaire : . . .

☐ Valider les paramètres en quittant

Avancé...

OK Annuler

Voulez-vous autoriser les autres pc de ce réseau a détecter votre pc → oui

Pour accéder à l'interface Web de pfSense on se rend dans son navigateur à l'adresse 192.168.1.54

Les identifiants par défaut de pfSense : id : admin / mdp : pfsense

Wizard / pfSense Setup / General Information ?

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname: srv-pfsense
EXAMPLE: myserver

Domain: home.arpa
EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server: 192.168.5.2

Secondary DNS Server:

Override DNS: ☒
Allow DNS servers to be overridden by DHCP/PPP on WAN

>> Next

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname: 2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.

Timezone: Europe/Paris

>> Next

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

Static IP Configuration

IP Address	192.168.5.54
Subnet Mask	24
Upstream Gateway	192.168.5.2

DHCP client configuration

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address	192.168.15.54
Type dhcp if this interface uses DHCP to obtain its IP address.	
Subnet Mask	24

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if e

Admin Password	*****
Admin Password AGAIN	Passw0rd

>> Next

On va dans firewall → Rules → OPT1(em2)

On active l'interface (enable)

Speed and Duplex: Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

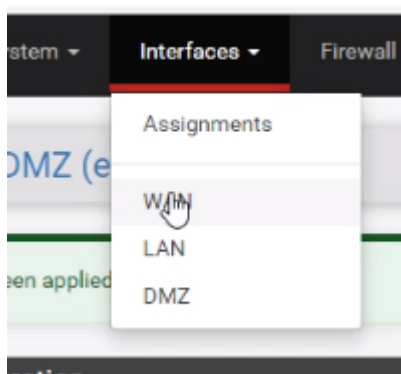
IPv4 Address	192.168.10.54	/ 24
IPv4 Upstream gateway	None	+ Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

Reserved Networks

On se retrouve avec nos 3 cartes

.15.54/interfaces.php?if=opt1



Voici la configuration rules de LAN pour l'instant

[Floating](#)
[WAN](#)
[LAN](#)
[DMZ](#)

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 0/3.04 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/> 8/1.17 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/> 0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add
 Add
 Delete
 Save
 Separator

COMMUNITY EDITION

Services / [DNS Resolver](#) / [General Settings](#)

[General Settings](#)
[Advanced Settings](#)
[Access Lists](#)

General DNS Resolver Options

Enable ☒ Enable DNS resolver

Listen Port

The port used for responding to DNS queries. It should normally be left blank unless another service needs it.

Enable SSL/TLS Service ☐ Respond to incoming SSL/TLS queries from local clients

Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients. This option disables automatic interface response routing behavior, thus it works best with specific interfaces.

SSL/TLS Certificate

The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.

SSL/TLS Listen Port

The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs it.

Network Interfaces

Interface IPs used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are used. If only one is selected, the other interface IPs not selected below are discarded. The default behavior is to respond to queries on every interface.

Outgoing Network Interfaces

Interface IPs used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are used. If only one is selected, the other interface IPs not selected below are discarded. The default behavior is to respond to queries on every interface.

On désactive les règles par défaut sur l'interface LAN

<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 *	LAN net	*	*	*	*	none	Default allow LAN to any rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv6 *	LAN net	*	*	*	*	none	Default allow LAN IPv6 to any rule	

Cependant on laisse activer la Rule Anti-lockout Rule car elle autorise l'adresse ip du firewall l'accès au port 443 et 80. Elle autorise n'importe quel client sur l'interface LAN à accéder à l'interface web à partir des ports

443 et 80.

On crée plusieurs règles qui permettront la sortie de la zone LAN vers : la résolution DNS, le PING, http, https vers "tout"

Les règles sont lues de haut en bas, on applique donc la règle DNS en haut de la liste

On ajoute donc 4 Rules en cliquant sur le bouton « add »

- Le protocole ICMP (test : ping 8.8.8.8 en cmd)
- Le port 53 pour la résolution de noms (DNS)
- Le port 80 et 443 (http/https)

Règle qui permet la sortie LAN vers la résolution DNS :

Action	Pass		
<small>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</small>			
Disabled	<input type="checkbox"/> Disable this rule <small>Set this option to disable this rule without removing it from the list.</small>		
Interface	LAN		
<small>Choose the interface from which packets must come to match this rule.</small>			
Address Family	IPv4		
<small>Select the Internet Protocol version this rule applies to.</small>			
Protocol	UDP		
<small>Choose which IP protocol this rule should match.</small>			
Source			
Source	<input type="checkbox"/> Invert match	LAN net	Source Address /
Display Advanced			
<small>The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.</small>			
Destination			
Destination	<input type="checkbox"/> Invert match	any	Destination Address /
Destination Port Range	DNS (53)	Custom	DNS (53) Custom
<small>Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.</small>			
Extra Options			
Log	<input type="checkbox"/> Log packets that are handled by this rule <small>Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).</small>		
Description	sortie_LAN_DNS <small>A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.</small>		
Advanced Options	Display Advanced		
Rule Information			

Règle qui permet la sortie LAN vers le PING

Action	Pass		
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.			
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	LAN		
Choose the interface from which packets must come to match this rule.			
Address Family	IPv4		
Select the Internet Protocol version this rule applies to.			
Protocol	ICMP		
Choose which IP protocol this rule should match.			
ICMP Subtypes	<div>any</div> <div>Alternate Host</div> <div>Datagram conversion error</div> <div>Echo reply</div>		
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.			
Source			
Source	<input type="checkbox"/> Invert match	LAN net	Source Address /
Destination			
Destination	<input type="checkbox"/> Invert match	any	Destination Address /
Extra Options			
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).		
Description	sortie_LAN_ping		
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.			
Advanced Options	<input type="button" value="Display Advanced"/>		
Rule Information			

Règle qui permet la sortie LAN vers le HTTP & l'HTTPS

Action

Pass

▼

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

▼

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

▼

Select the Internet Protocol version this rule applies to.

Protocol

TCP

▼

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

LAN net

▼

Source Address

/

▼

⚙ Display Advanced

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination

☐ Invert match

any

▼

Destination Address

/

▼

Destination Port Range

HTTPS (443)

▼

From

Custom

HTTPS (443)

▼

To

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

sortie_LAN_https

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

⚙ Display Advanced

Rule Information

Action	Pass		
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.			
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	LAN		
Choose the interface from which packets must come to match this rule.			
Address Family	IPv4		
Select the Internet Protocol version this rule applies to.			
Protocol	TCP		
Choose which IP protocol this rule should match.			
Source			
Source	<input type="checkbox"/> Invert match	LAN net	Source Address /
<input type="button" value="Display Advanced"/> <p>The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.</p>			
Destination			
Destination	<input type="checkbox"/> Invert match	any	Destination Address /
Destination Port Range	<input type="text" value="HTTP (80)"/> <input type="text" value="Custom"/>	<input type="text" value="HTTP (80)"/> <input type="text" value="Custom"/>	
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.			
Extra Options			
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).		
Description	sortie_LAN_http A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.		
Advanced Options	<input type="button" value="Display Advanced"/>		
Rule Information			

On télécharge une iso Ubuntu mini

On la connecte au segment LAN-DMZ qui correspond à notre réseau pour le serveur web

On configure le fichier 01.netcfg.yaml dans etc/netplan en désactivant le DHCP (pas de DHCP pour les serveurs). On lui attribue une adresse IP, une gateway et un DNS

```
GNU nano 2.9.3 /etc/netplan/01-netcfg.yaml

# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:
  version: 2
  renderer: networkd
  ethernets:
    ens33:
      dhcp4: no
      dhcp6: no
      addresses: [192.168.10.11/24]
      gateway4: 192.168.10.54
      nameservers:
        addresses: [192.168.10.54]

[ Défilement progressif - marche ]
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^J Justifier  ^C Pos. cur.  M-U Annuler
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^T Orthograp.^_ Aller lig. M-E Refaire
```

Pour autoriser l'accès au port 81 du serveur Web, on doit spécifier en plus l'écoute au port 81 directement dans le fichier port.conf d'Apache

```
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80
Listen 81

<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

root@ubuntu:/etc/apache2# systemctl restart apache2
root@ubuntu:/etc/apache2#
```

On applique les changements avec `systemctl restart apache2`

Pour pouvoir accéder à Internet, il faudra dans pfSense ajouter une nouvelle règle :

Firewall → Rules → OPT1 : protocol : any ; from any to any

Dans le serveur web on applique les changements : `sudo netplan apply`

On met tout à jour avec `apt-get update`

Nous allons désormais installer Apache2 pour mettre en place notre serveur

On exécute `apt install apache2`

On configure le fichier de conf dans `/etc/apache2/sites-available`

On y ajoute le port et le ServerName.

```
<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
ServerName site0.contoso.web

ServerAdmin webmaster@localhost
DocumentRoot /var/www/80

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

kssb@ubuntu:~$
```

On fait de même pour site1.contoso.web sur le port 81

On interdit l'accès à la zone DMZ vers la zone LAN grâce à la règle suivante que l'on applique à partir du LAN vers OPT1 et on autorise les requêtes du port 80,53, 443 ainsi que les requête ICMP

Edit Firewall Rule

Action

Reject

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

OPT1

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match










































any

Source Address

/

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Rules (Drag to Change Order)												
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input type="checkbox"/>	 0 / 0 B	IPv4 TCP	*	*	*	*	*	none			    	
<input type="checkbox"/>	 0 / 0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			    	
<input type="checkbox"/>	 0 / 0 B	IPv4 UDP	*	*	*	53 (DNS)	*	none			    	
<input type="checkbox"/>	 0 / 0 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			    	
<input type="checkbox"/>	 0 / 9.44 MiB	IPv4 *	*	*	*	*	*	none			    	
<input type="checkbox"/>	 0 / 0 B	IPv4 ICMP any	*	*	*	*	*	none			    	
								 Add	 Add	 Delete	 Save	 Separator

On ajoute une règle qui permettra l'accès depuis la zone LAN aux ports 80 et 81 du serveur Web

Pour le port 80 :

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

any

Source Address /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination

☐ Invert match

any

Destination Address /

Destination Port Range

HTTP (80)

From

Custom

HTTP (80)

To

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

aces_80_LAN

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Et pour le port 81 :

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

any

Source Address

/

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination

☐ Invert match

any

Destination Address

/

Destination Port Range

(other)

81

(other)

81

From

Custom

To

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description

aces_81_LAN

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Edit Firewall Rule			
Action	<div>Pass</div> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</p>		
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	<div>LAN</div> <p>Choose the interface from which packets must come to match this rule.</p>		
Address Family	<div>IPv4</div> <p>Select the Internet Protocol version this rule applies to.</p>		
Protocol	<div>TCP</div> <p>Choose which IP protocol this rule should match.</p>		
Source			
Source	<input type="checkbox"/> Invert match	<div>any</div>	<div>Source Address</div> / <div></div>
<div>Display Advanced</div> <p>The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.</p>			
Destination			
Destination	<input type="checkbox"/> Invert match	<div>any</div>	<div>Destination Address</div> / <div></div>
Destination Port Range	<div>(other)</div>	<div>81</div>	<div>(other)</div> <div>81</div>
	From	Custom	To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.			
Extra Options			
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).		
Description	<div>acces_81_LAN</div> <p>A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.</p>		

Nous allons désormais installer et configurer le service SquidGuard qui va nous permettre la gestion du blocage de noms de domaine et URL

Il faudra tout d'abord installer les packages « squid » et « squidGuard »

On se rend dans System → Package Manager → Availables Packages

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term Both

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description	
Lightsquid	3.0.6_8	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package. Package Dependencies: lighttpd-1.4.58 lightsquid-1.8_5	<input type="button" value="+ Install"/>
squid	0.4.45_3	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP. Package Dependencies: squidclamav-7.1 squid_radius_auth-1.10 squid-4.13 c-icap-modules-0.5.4	<input type="button" value="+ Install"/>
squidGuard	1.16.18_18	High performance web proxy URL filter. Package Dependencies: squidguard-1.4_15	<input type="button" value="+ Install"/>

On accède ensuite au SquidProxyServer dans l'onglet général pour l'activer.

Package / Proxy Server: General Settings / General

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Auth

Squid General Settings

Enable Squid Proxy ☒ Check to enable the Squid proxy.
Important: If unchecked, ALL Squid services will be disabled and stopped.

On active le SquidGuard Proxy Filter pour pouvoir filtrer certains URL.

Package / Proxy filter SquidGuard: General settings / General settings

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync

General Options

Enable ☒ Check this option to enable squidGuard.
Important: Please set up at least one category on the 'Target Categories' tab before enabling. See [this link for details](#).
The Save button at the bottom of this page must be clicked to save configuration changes.
To activate squidGuard configuration changes, **the Apply button must be clicked.**

SquidGuard service state: **STOPPED**

Pour gérer le blocage d'URL à partir d'une blacklist, on se rend dans « Services → SquiGuard Proxy Filter → Blacklist »

Activer « Enable Blacklist » et insérer dans BlackList URL: http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

Blacklist options

Blacklist

☒ Check this option to enable blacklist
Do NOT enable this on NanoBSD installs!

Blacklist proxy

Blacklist upload proxy - enter here, or leave blank.
Format: host:[port login:pass] . Default proxy port 1080.
Example: '192.168.0.1:8080 user:pass'

Blacklist URL

Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or leave blank. The LOCAL path could be your pfsense (/tmp/blacklist.tar.gz).

Save

Dans l'onglet « Blacklist », on clique sur « Download » pour télécharger la liste de filtrage.

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Package / SquidGuard / Blacklists

General settings

Common ACL

Groups ACL

Target categories

Times

Rewrites

Blacklist

Log

XMLRPC Sync

Blacklist Update

Blacklist DB rebuild progress

1 %

Download

Cancel

Restore Default

Enter FTP or HTTP path to the blacklist archive here.

Blacklist update Log

```

Begin blacklist update
Start download.
Download archive http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz
Download complete
Unpack archive
Scan blacklist categories.
Found 58 items.
Start rebuild DB.
Copy DB to workdir.
Reconfigure Squid proxy.
Blacklist update complete.

```

Dans l'onglet « Common ACL », on clique sur « Target Rules List » sur le « + » puis on sélectionne les catégories à bloquer et on sélectionne « allow » pour « default access [all] »

[blk_blacklists_liste_bu]	access	—	▼
[blk_blacklists_malware]	access	—	▼
[blk_blacklists_manga]	access	—	▼
[blk_blacklists_marketingware]	access	—	▼
[blk_blacklists_mixed_adult]	access	—	▼
[blk_blacklists_mobile-phone]	access	—	▼
[blk_blacklists_phishing]	access	—	▼
[blk_blacklists_press]	access	—	▼
[blk_blacklists_publicite]	access	—	▼
[blk_blacklists_radio]	access	—	▼
[blk_blacklists_reaffected]	access	—	▼
[blk_blacklists_redirector]	access	—	▼
[blk_blacklists_remote-control]	access	—	▼
[blk_blacklists_sect]	access	—	▼
[blk_blacklists_sexual_education]	access	—	▼
[blk_blacklists_shopping]	access	—	▼
[blk_blacklists_shortener]	access	—	▼
[blk_blacklists_social_networks]	access	—	▼
[blk_blacklists_special]	access	—	▼
[blk_blacklists_sports]	access	—	▼
[blk_blacklists_strict_redirector]	access	—	▼
[blk_blacklists_strong_redirector]	access	—	▼
[blk_blacklists_translation]	access	—	▼
[blk_blacklists_tricheur]	access	—	▼
[blk_blacklists_update]	access	—	▼
[blk_blacklists_warez]	access	—	▼
[blk_blacklists_webmail]	access	—	▼
Default access [all]	access	allow	▼

Nous allons devoir créer une GPO pour configurer le proxy de Mozilla Firefox et Microsoft Edge

Pour Microsoft Edge on se rend dans les options de proxy du navigateur :

Accueil

Réseau et Internet

État

Ethernet

Accès à distance

VPN

Proxy

Proxy

☒ Activé

Utiliser un script d'installation

☐ Désactivé

Adresse du script

Configuration manuelle du proxy

Utilisez un serveur proxy pour les connexions Ethernet ou Wi-Fi. Ces paramètres ne s'appliquent pas aux connexions VPN.

Utiliser un serveur proxy

☒ Activé

Adresse

192.168.15.54

Port

3128

Puis nous allons télécharger et installer des stratégies liées au navigateur Firefox :

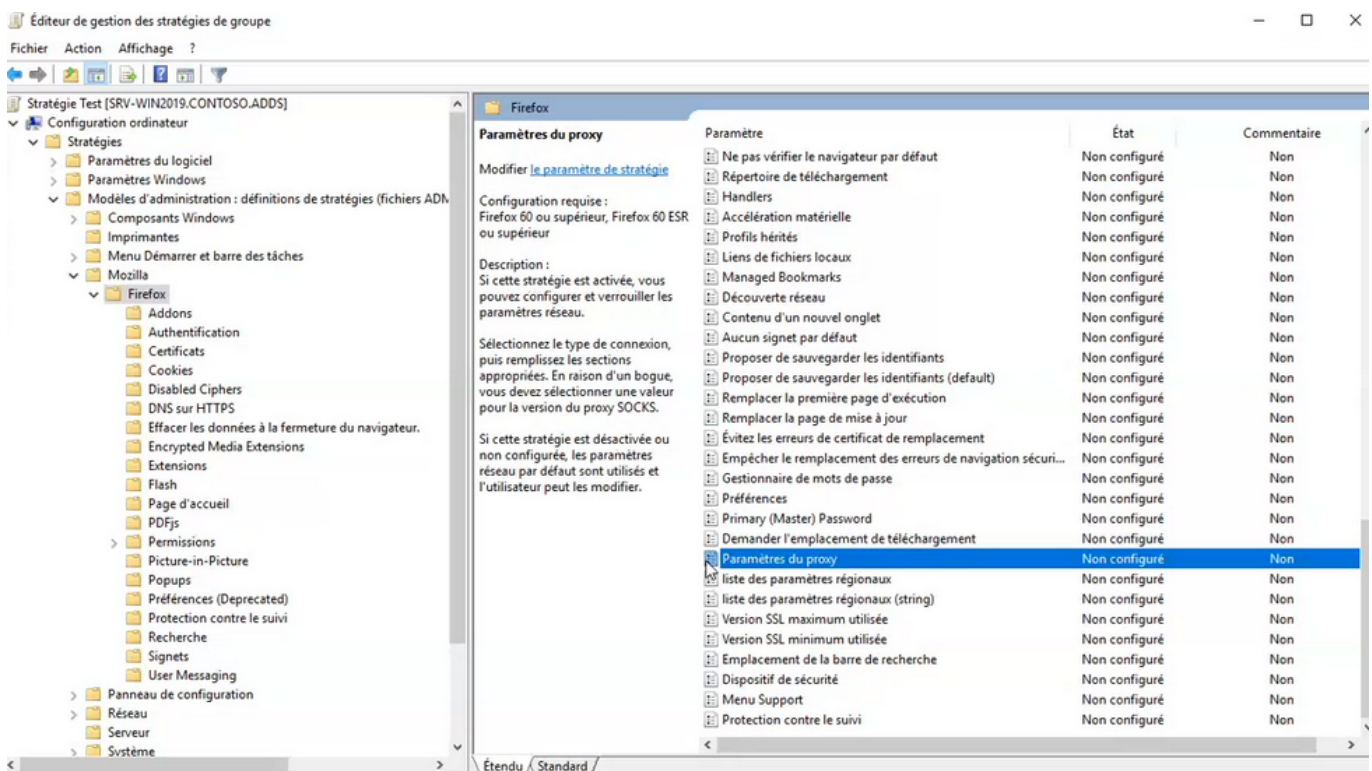
Pour cela, nous nous rendons sur le site : <https://github.com/mozilla/policy-templates/releases> et télécharger le fichier Policy_templates_v2.10.zip

Ensuite nous allons dans C:\Windows\ et nous copions le dossier PolicyDefinitions et nous le collons dans D:\ADDS\SYVOL\domain\Policies\PolicyDefinitions

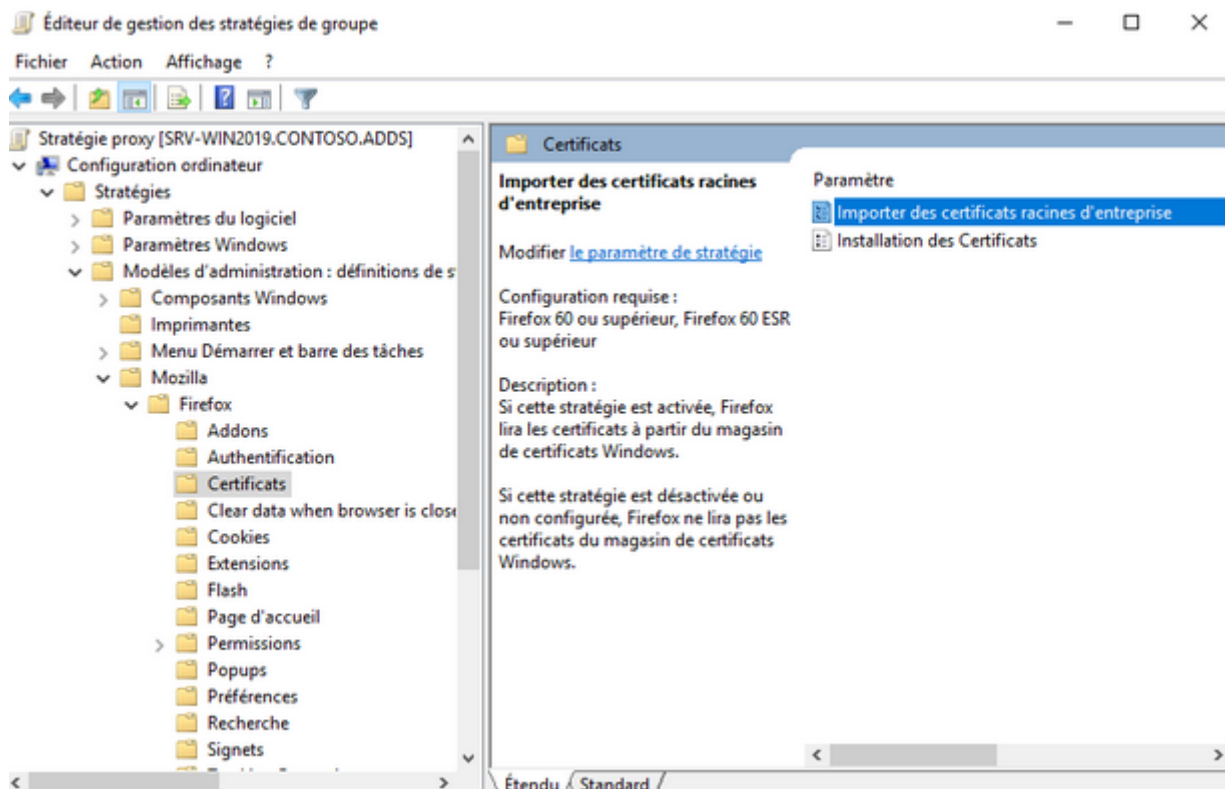
Puis nous copions les dossiers fr-FR, en-US, les fichiers mozilla.admx et firefox.admx de l'archive dans le dossier PolicyDefinition



Dans les paramètres de notre stratégie de groupe, le dossier Mozilla apparaît, on peut alors activer les paramètres de proxy :



Nous allons ensuite créer une GPO qui va gérer le "push" du certificat racine de pfSense sur les postes clients



Question légalité : est-il acceptable d'intercepter le trafic https ? Quel est le nom et le fonctionnement de cette méthode ?

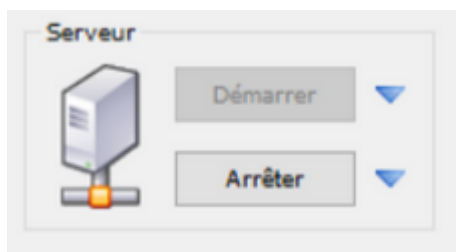
Il est possible de contrôler le contenu des données échangées entre le client et le serveur afin de s'assurer que les flux HTTPS ne sont pas utilisés pour faire sortir du système d'information des données confidentielles. Cependant le contrôle de données n'est pas toujours utilisé de cette manière. Certaines personnes utilisent ce fonctionnement pour récupérer des informations personnelles etc.

Le fonctionnement de cette méthode se nomme : man-in-the-middle.

Nous allons désormais configurer l'utilisation de Squid sur les postes clients avec WPAD.

Un serveur Web peut être monté sur la zone LAN, il fonctionnera sur le port 80 et hébergera à sa racine un fichier « wpad.dat ».

Tout d'abord il faut créer un serveur web avec UWAMP qui hébergera ce fichier puis démarrer le serveur



Nous allons maintenant créer une règle DNS pour servir le fichier à l'adresse : wpad.contoso.adds

On crée donc un hôte dans la zone de recherche directe contoso.adds, avec l'extension wpad pointant sur notre serveur.

Nouvel hôte

Nom (utilise le domaine parent si ce champ est vide) :

wpad

Nom de domaine pleinement qualifié (FQDN) :

wpad.contoso.adds.

Adresse IP :

192.168.15.11

☐ Créer un pointeur d'enregistrement PTR associé

☐ Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire

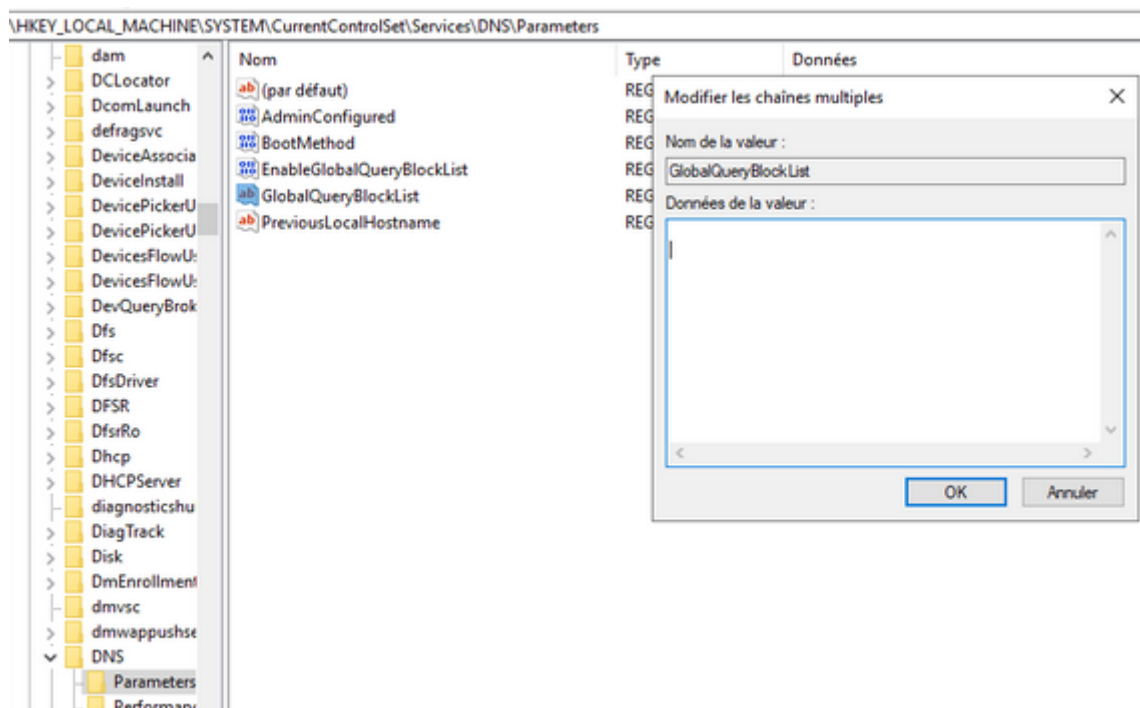
Ajouter un hôte Annuler

Il faut désormais vider le regedit. On lance l'invite de commande en tant qu'administrateur et on exécute la commande suivante :

- Dnscmd /info /globalqueryblocklist

Puis on supprime les valeurs du regedit à l'emplacement :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters\GlobalQueryBlockList



Pour vider le cache, on lance l'invite de commande en administrateur et on exécute la commande suivante :

- ipconfig /flushdns

Nous allons désormais créer un fichier wpad.dat dans lequel nous allons définir et configurer le proxy.

Ce fichier sera servi par le serveur Uwamp et permettra de configurer les navigateurs clients

```
function FindProxyForURL(url, host)
{
    if (dnsDomainIs(host, « contoso.adds »))
    {
        return « DIRECT »;
    }
    else
    {
        return « PROXY 192.168.15.54:3128 »;
    }
}
```

Nous allons maintenant configurer le Reverse Proxy.

Pour se faire, nous devons rediriger les sous domaines site0.contoso.web et site1.contoso.web vers le serveur web respectivement sur les ports 80 et 81.

Nous allons activer Squid Reverse Proxy sur l'interface WAN.

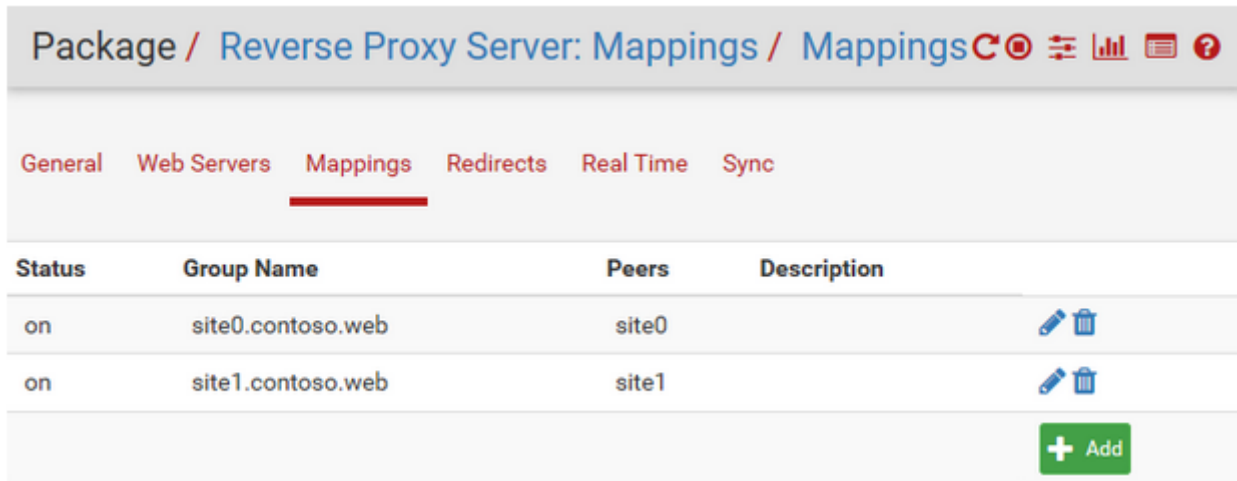
Pour ajouter nos 2 sites, il faut avant tout les ajouter dans « Web Servers » en précisant l'IP de destination de notre serveur web à l'adresse IP : 192.168.10.11 et les ports affectés : 80 puis 81

Status	Alias	IP Address	Port	Protocol	Description
on	site0	192.168.10.11	80	HTTP	Site 80
on	site1	192.168.10.11	81	HTTP	Site 81

[+ Add](#)

[Save](#)

Nous allons également utiliser des alias pour ajouter nos 2 serveurs dans des groupes et leur spécifier une URL dans Mappings afin qu'il continue de réaliser son rôle.

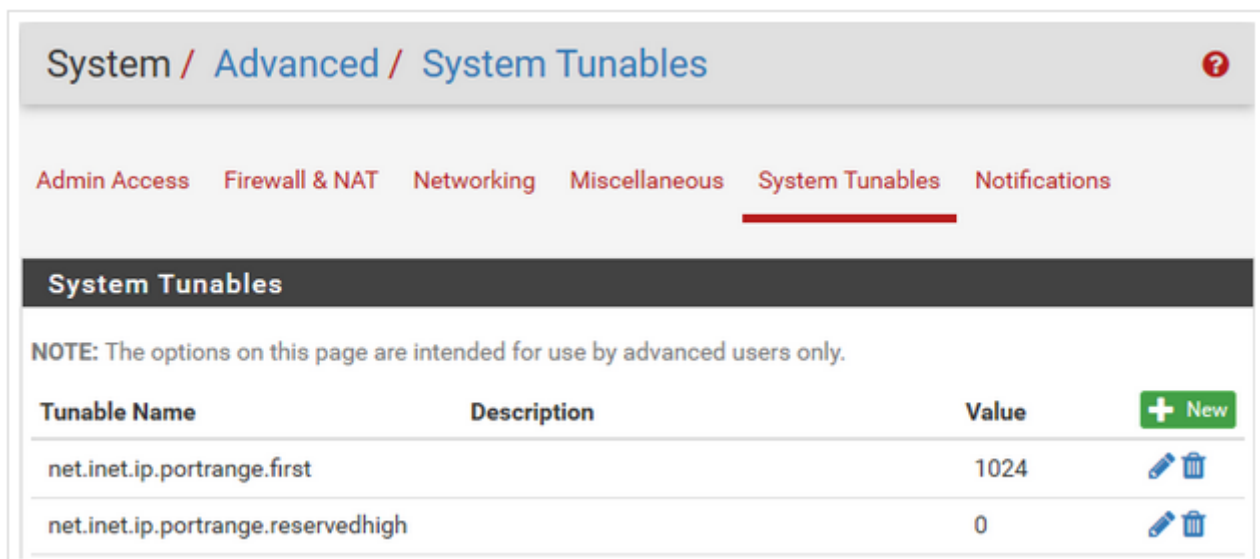


Nous devons aussi rediriger les requêtes que l'on va recevoir.

Nous modifions donc le fichiers hosts dans /etc/hosts :

```
127.0.0.1    localhost
127.0.1.1    srv-web.localdomain    srv-web
127.0.0.1    site0.contoso.web
127.0.0.1    site1.contoso.web
# The following lines are desirable for IPv6 capable hosts
```

Il faut maintenant activer le « reverse proxy http » sur le port 80. Pour cela il faut modifier le port minimum qui est demandé pour le reverse proxy. Il faut donc ajouter une nouvelle « Tunables » nommé « **net.inet.ip.portrange.reservedhigh** » et mettre la valeur à 0



Pour tester le Reverse Proxy, nous allons accéder à « C:\Windows\System32\drivers\etc ».

Nous allons déplacer le fichier hosts en dehors de son dossier car nous n'avons pas les droits d'édition, et nous allons rajouter à l'intérieur l'ip de notre serveur web. Il faudra ensuite le remplacer par le fichier original présent dans le dossier.

On peut désormais ping www.contoso.web sans problème et accéder à nos sites web sans problème.



Problèmes rencontrés :

Il est primordial de vider le cache avec la commande « `ipconfig /flushdns` » après avoir supprimé les valeurs du regedit afin que les changements soient pris en compte.