Titre	Installation et configuration d'une CA sous Windows Server 2008
Propriétaire	Tavares José
Classification	Interne
Date dernière	28 Septembre 2009
modification	
Chemin\NomFichier	\\10.1.1.1\FilesTD\Group4\Personnel\Tavares\00 EIG\CA LaboTD.doc

## CA MICROSOFT SOUS WINDOWS SERVER 2008......1

0	But	. 1
1	Installation de Windows Server 2008	. 2
2	Installation d'une CA	. 3
3	Accepter automatiquement les requêtes de certificats	. 8
4	Configuration IP, login et mot de passe	. 8
5	Configurer les chemins de CRL et AIA	. 9
6	Se faire délivrer un certificat serveur	10
7	Configurer le DNS	14
8	Configuration du firewall Clavister	15

### CA Microsoft sous Windows Server 2008

### 0 But

Configurer l'autorité de certification (CA) **LaboTD** à partir de Windows Server 2008 ; mises à jour des configurations DNS et firewall Clavister

Remarques

- Utilisation d'une architecture virtualisée ESXi 4 (PC-G16)
- Accès depuis <u>http://ca.tdeig.ch</u>

### 1 Installation de Windows Server 2008

Une installation par défaut a été faite, sur une base Windows Server 2008 64bits Standard Edition

Cette installation c'est effectuée dans une machine virtuelle, sur un disque virtuel de 20GB, et a nécessité environ 45minutes

Après installation, l'écran d'accueil est le suivant

<b>E</b> Initia	Configuration Lasks		
	Perform the following tasks to initially configu	re this server	Standard Windows Server 2008
	Provide Computer Information		Specifying computer information
	Set time <u>z</u> one	Time Zone:	(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
	Configure networking	Local Area Connection:	Assigned by DHCP
	Novide computer name and domain	Full Computer Name: Workgroup:	WIN2008-CA WORKGROUP
	2 Update This Server		Updating your Windows server
	Enable automatic updating and feedback	Updates: Feedback:	Not configured Windows Error Reporting off Not participating in Customer Experience Improvement Program
	Download and install updates	Checked for Updates: Installed Updates:	Never
	3 Customize This Server		Customizing your server
	Add roles	Roles:	Active Directory Certificate Services, Web Server (IIS)
	Add features	Features:	Remote Server Administration Tools, Windows Process Activation Service
	Enable Remote Des <u>k</u> top	Remote Desktop:	Disabled
	Configure Windows Firewall	Firewall:	Off
	$Print, e\text{-mail}, or \underline{s} ave this information$		
Q.	Do not show this window at logon		Qose

# 2 Installation d'une CA

Cliquer sur Add roles puis sélectionner Active Directory Certificate Services, ainsi que Web Server (IIS)

Add Roles Wizard		×
Select Server Ro	les	
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Web Server (IIS) Role Services Confirmation Progress Results	Select one or more roles to install on this server.         Roles: <ul> <li>Active Directory Certificate Services</li> <li>Active Directory Domain Services</li> <li>Active Directory Federation Services</li> <li>Active Directory Rights Management Services</li> <li>Active Directory Rights Management Services</li> <li>Application Server</li> <li>DHCP Server</li> <li>DNS Server</li> <li>Fax Server</li> <li>Hyper-V</li> <li>Network Policy and Access Services</li> <li>Print Services</li> <li>UDDI Services</li> <li>Web Server (IIS)</li> <li>Windows Deployment Services</li> </ul> More about server roles	Description:         Active Directory Certificate Services         (AD CS) is used to create certification         authorities and related role services         that allow you to issue and manage         certificates used in a variety of         applications.

Le serveur web IIS est en effet nécessaire pour faire des demandes de certificats à notre CA

Sélectionner les 2 champs ci-dessous (*Certification Authority Web Enrollment* est nécessaire afin de pouvoir faire des requêtes de certificat via IIS)

Add Roles Wizard	
Select Role Servi	ces
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Web Server (IIS) Role Services Confirmation Progress Results	Select the role services to install for Active Directory Certificate Services:       Description:         ✓ Certification Authority       Certification Authority Web Enrolment       Certification Authority Web Enrolment         ✓ Certification Authority Web Enrolment       Certification Authority Web Enrolment       Certification Authority Web Enrolment         ✓ More about role services       Certification Authority Web Enrolment       Certificate revocation lists (CRLs), and enroll for smart card certificates.

### Sélectionner Standalone

Add Roles Wizard		×
Specify Setup Ty	pe	
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Web Server (IIS) Role Services Confirmation Progress Results	<ul> <li>Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.</li> <li>C Enterprise Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.</li> <li>C Standalone Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.</li> </ul>	
	< Previous Next > Install Cancel	

### Il s'agit d'une Root CA :



### Sélectionner Create a new private key

Add Roles Wizard	×
Set Up Private Ke	ε <b>γ</b>
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Web Server (IIS) Role Services Confirmation Progress Results	<ul> <li>To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one.</li> <li>Create a new private key</li> <li>Use this option if you don't have a private key or wish to create a new private key to enhance security. You will be asked to select a cryptographic service provider and specify a key length for the private key. To issue new certificates, you must also select a hash algorithm.</li> <li>Use this option to ensure continuity with previously issued certificates when reinstalling a CA.</li> <li>Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.</li> <li>Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.</li> <li>Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.</li> <li>Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.</li> </ul>
	More about public and private keys
	< Previous Next > Install Cancel

### hepia - Labo de transmission de données -5-

Choisir de créer une clé **RSA de 4096 bits** avec **sha1** comme algorithme de hash

Configure Cryptography for CA						
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Web Server (IIS) Role Services Confirmation Progress	To create a new private key, you must first select a <u>cryptographic service provider</u> , <u>hash algorithm</u> , and key length that are appropriate for the intended use of the certificates that you issue. Selecting a higher value for key length will result in stronger security, but increase the time needed to complete signing operations. Select a cryptographic service provider (CSP): RSA #Microsoft Software Key Storage Provider Select the hash algorithm for signing certificates issued by this CA: sha1 md2 md4 md4 uff Use strong private key protection features provided by the CSP (this may require administrator interaction every time the private key is accessed by the CA)					
Results	More about cryptographic options for a CA         < Previous					

### Notre CA va s'appeler LaboTD

Add Roles Wizard		<u> </u>
Configure CA Na	me	
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography	Type in a common name to identify this CA. This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified. <u>Common name for this CA:</u> [LaboTD] <u>Distinguished name suffix:</u>	
CA Name	Preview of distinguished name:	
Validity Period Certificate Database Web Server (IIS) Role Services Confirmation Progress Results	CN=LaboTD	
	More about configuring a CA name	
	< <u>Previous</u> <u>Next</u> > <u>Install</u> Cancel	

### Le certificat root aura une validité de 10 ans :



Laisser les options suivantes par défaut, puis un résumé nous sera présenté :

Confirm Installat	tion Selections		_
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Web Server (IIS) Role Services <b>Confirmation</b> Progress Results	To install the following roles, role servic	es, or features, click Install. ges below tarted after the installation completes. ervices of this computer cannot be changed after Certification Authority Standalone Root RSA #Microsoft Software Key Storage Provider sha 1 4096 Disabled 07.09,2019 12:56 CN=LaboTD C:\Windows\system32\CertLog C:\Windows\system32\CertLog C:\Windows\system32\CertLog rollment System Resource Manager (WSRM) and how it can help optimize	
	Print, e-mail, or save this information	< Previous Next > Install Cancel	

### hepia - Labo de transmission de données -7-

Start – Administrative Tools – Certification Authority File Action View Help 🙀 Certification Authority (Local) Description Name 🗆 🦼 LaboTD d LaboTD Certification Authority 📔 Revoked Certificates Issued Certificates Pending Requests 📔 Failed Requests

# La CA peut ensuite être administrée sur le serveur, sous

#### 3 Accepter automatiquement les requêtes de certificats

Start – Administrative Tools – Certification Authority

Clic-droit sur la CA - Properties - Onglet Policy Module - Properties...

Sélectionner la valeur ci-dessous



OK

Redémarrer la CA pour appliquer les changements

#### 4 Configuration IP, login et mot de passe

```
Adresse IP
            = 129.194.184.89
            = 255.255.252.0
Netmask
Gateway
            = 129.194.184.1
            = 129.194.184.84 - 129.194.4.6
DNS
Login = Administrator
Pass = carte CryptMe
```

### 5 Configurer les chemins de CRL et AIA

Par défaut, les chemins de **CRL** (*Certificate Revocation List*) et AIA (*Authority Information Access*) sont désignés par le nom PC ou s'exécute la CA. Le paramètre AIA pointe en réalité sur le certificat root de la CA

Dans notre cas, il a fallu reconfigurer ces chemins dans la CA : *Start – Administrative Tools – Certification Authority* 

Clic-droit sur la CA – Properties – Onglet Extensions

Effectuer un Remove des 2 dernières entrées (http://... et file://...)

Storage	Storage Auditing Security					
General Policy Module Exit Module Extensions					Extensions	
Select extensi	on:					
CRL Distributi	ion Point (	CDP)			-	
Specify locatio (CRL).	ins from w	hich users ca	in obtain a cer	tificate re	vocation list	
C:\Windows\ Idap:///CN=< http:// <server< th=""><th>system 32 CATrunca rDNSNan DNSNam</th><th>VCertSrv/Cert atedName&gt;&lt;0 ne&gt;/CertEnrol a&gt;/CertEnroll.</th><th>Enroll\<cana CRLNameSuffi I/<caname>&lt; /<caname>&lt;(</caname></caname></cana </th><th>me&gt;<cri x&gt;,CN=&lt; CRLNam CRLName</cri </th><th>LNameSuffix&gt;&lt; ServerShortNar heSuffix&gt;<delta eSuffix&gt;<deltac< th=""></deltac<></delta </th></server<>	system 32 CATrunca rDNSNan DNSNam	VCertSrv/Cert atedName><0 ne>/CertEnrol a>/CertEnroll.	Enroll\ <cana CRLNameSuffi I/<caname>&lt; /<caname>&lt;(</caname></caname></cana 	me> <cri x&gt;,CN=&lt; CRLNam CRLName</cri 	LNameSuffix>< ServerShortNar heSuffix> <delta eSuffix&gt;<deltac< th=""></deltac<></delta 	
•					F	
			Add	I	Remove	
Publish CF	Ls to this	location				
Include in when publ	Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.					
🔲 Include in	Include in CRLs, Clients use this to find Delta CRL locations.					
Include in the CDP extension of issued certificates						
Publish Delta CRLs to this location						
Include in the IDP extension of issued CRLs						
	ОК	Can	cel /	Apply	Help	

Puis à l'aide du bouton *Add...*, ajouter la bonne url sans oublier de cocher les 2 cases <u>comme ci-dessous :</u>

LaboTD Propert	ties			<u>?</u> ×
Storage General	AL Policy Module	uditing Exit Modu	Jle	Security Extensions
Select extensi	on:			
CRL Distributi	ion Point (CDP)			▼
Specify locatio (CRL).	ons from which users o	an obtain a cer	tificate rev	vocation list
C:\Windows\ Idap:///CN=<	system32\CertSrv\Ce <catruncatedname></catruncatedname>	rtEnroll\ <canar <crlnamesuffi< th=""><th>ne&gt;<crli x&gt;,CN=<s< th=""><th>NameSuffix&gt;&lt;1 ierverShortNar</th></s<></crli </th></crlnamesuffi<></canar 	ne> <crli x&gt;,CN=<s< th=""><th>NameSuffix&gt;&lt;1 ierverShortNar</th></s<></crli 	NameSuffix><1 ierverShortNar
http://ca.tdei	ig.ch/CertEnroll/Labo	TD.crl		
•				▶
		Add		Remove
🗖 Publish CF	RLs to this location			
Include in when publ	all CRLs. Specifies w lishing manually.	here to publish i	n the Activ	ve Directory
Include in	CRLs. Clients use this	to find Delta Cf	RL location	ns.
🔽 Include in f	the CDP extension of	issued certificat	es	
🔲 Publish De	elta CRLs to this locat	on		
Include in t	the IDP extension of i	ssued CRLs		
	OK Ca	ncel /	Apply	Help

### Source

http://technet.microsoft.com/en-us/library/cc773036(WS.10).aspx

### 6 Se faire délivrer un certificat serveur

### Remarques importantes (problèmes rencontrés)

La durée de vie du certificat a été modifiée à 9 ans <u>http://support.microsoft.com/kb/254632/</u> Puis redémarrer la CA (Clic droit sur la CA – *All tasks* – Stop...)

Lors d'une demande de certificat depuis un poste Vista exécutant IE7, on obtient une erreur :

An error occurred while creating the certificate request. Please verify that your CSP supports any settings you have made and that your input is valid. Suggested cause: No suggestion. Error: 0x80070005 - (unknown)

Ceci se produit car IE7 est lancé avec peu de privilèges sous Vista, ce problème a été corrigé avec IE8 qui fonctionne déjà différemment.

Il est cependant possible de résoudre cette erreur sous IE7, en ajoutant le site web de la CA à la zone *Trusted sites* Lorsqu'un essaie d'ouvrir un site faisant partie de la zone *Trusted*, IE7 lance une nouvelle

Lorsqu'un essaie d'ouvrir un site faisant partie de la zone *Trusted*, IE7 lance une nouve fenêtre avec des privilèges différents, ce qui résout le problème !

Sources :

http://social.technet.microsoft.com/Forums/en-US/itprovistaie/thread/75b0450e-4926-47df-8885-b8e209919c16 http://support.microsoft.com/kb/922706/en-us

Tools - Internet Options - Security - Trusted sites



### Cliquer sur le bouton Sites

Décocher la case *Require server verification (https:) for all sites in this zone* Ajouter le site web de la CA <u>http://ca.tdeig.ch</u>



Close – OK

Puis ouvrir http://ca.tdeig.ch avec IE7

On obtient l'avertissement suivant :

Interne	t Explorer	X
	Internet Explorer needs to open a new window to display this webpage.	
	For your computer's security, websites that are in different security zones must open in different windows.	n
	Do not show this message again	OK

Il ne reste plus qu'à autoriser les contrôles ActiveX (voir ci-dessous) pour la zone Trusted sites !

Cela est d'ailleurs préférable d'un point de vue sécurité, plutôt que d'autoriser pour tous les sites web ces contrôles ActiveX qui ne sont pas marqués comme sûrs !!

*Tools – Internet Options – onglet Security – Trusted sites - Custom level...* Modifier les valeurs ci-dessous :

	Display video and animation on a webpage that does not use	
	Disable	
	Enable	
	Download signed ActiveX controls	
	Disable	
	Enable	
	Prompt	
	Download unsigned ActiveX controls	
	Disable	
	Enable	
	Prompt	
	Initialize and script ActiveX controls not marked as safe for signal provide the provide the provide the provided as safe for signal provided as for sinclust provided as safe for signal provided	
	Disable     Eachla	
	Promot	
L	Only allow approved domains to use ActiveX without prompt	Ŧ
- L	4 III	
•	kes effect after you restart Internet Explorer	
∢ ( Tak		
∢ ( Tak		
∢ Tak set	t custom settings	
Tak set	t custom settings t to: Medium (default)	
∢ Tak set set	t custom settings t to: Medium (default)   Reset	

hepia - Labo de transmission de données -11-

### Création du certificat serveur

L'objectif est de créer une connexion SSL (https) sur le site web de la CA, et pour cela on a besoin de se faire délivrer un certificat serveur.

On va donc demander à la CA (nommée LaboTD) de nous délivrer un certificat serveur que l'on puisse associer à notre site web

Cette opération a pu se faire depuis le navigateur du serveur (ici c'est le même PC que la CA), en se connectant sur <u>http://localhost/certsrv</u> (ajouter ce site dans la zone *Trusted* et activer les contrôles ActiveX, voir pages 10-11)

Cliquer sur Request a certificate – advanced certificate request – Create and submit a request to this CA

On obtient le formulaire ci-dessous que l'on doit compléter (le champ Name est nécessaire) :

C Microsoft Active Directory Certificate Services - Windows Internet Explorer
C C + Martin http://localhost/certsrv/certrqma.asp
😭 🍪 🍘 Microsoft Active Directory Certificate Services
🕐 Internet Explorer has blocked this site from using an ActiveX control in an unsafe manner. As a result, this page may not display correctly.
Microsoft Active Directory Certificate Services tdeig.ch
Advanced Cartificate Doguest
Identifying Information:
Name:
E-Mail:
Company:
Department:
City:
State:
Country/Region:
Type of Certificate Needed:
Server Authentication Certificate
Key Options:
Key Usage: • Exchange • Signature • Both
Key Size: 0 Max: (common key sizes: )
Automatic key container name     O User specified key container name
☐ Mark keys as exportable —
Enable strong private key protection
Additional Options:
Request Format:  CMC CPKCS10
Hash Algorithm:
Only used to sign request.
Save request

Dans le champ Type of Certificate Needed, choisir Server Authentication Certificate

C Microsoft Active Directory Certificate Services - Windows Internet Explorer
🚱 🕢 👻 🙋 http://ocalhost/certsrv/certrqma.asp
😭 🍪 🏉 Microsoft Active Directory Certificate Services
Microsoft Active Directory Certificate Services tdeig.ch
Advanced Cartificate Request
Avanceu Certificate Request
Identifying Information:
Name:
E-Mail:
Company:
Department:
City:
State:
Country/Region:
Type of Certificate Needed:
Server Authentication Certificate
Key Options:
Create new key set C Use existing key set
CSP: Microsoft Enhanced RSA and AES Cryptographic Provider
Key Usage: O Exchange O Signature 💿 Both
Key Size: 1024 Min: 384 (common key sizes: <u>512 1024 2048 4096 8192 16384</u> )
• Automatic key container name • User specified key container name
☐ Mark keys as exportable
Enable strong private key protection
Additional Options:
Request Format:  CMC CPKCS10
Hash Algorithm: sha1 💌
Only used to sign request.
Save request

Cliquer sur submit pour soumettre la demande à la CA

### 7 Configurer le DNS

Se connecter au DNS debian via par exemple vShere Client (IP=10.1.1.52) Modifier le fichier **/etc/bind/db.tdeig** 

```
Attention, les espaces sont des TAB :
```

```
;
; BIND data file for tdeig.ch
;
$TTL
      604800
0
       IN
             SOA
                    nsl.tdeig.ch. root.tdeig.ch. (
  6
              ; Serial
                      604800
                                   ; Refresh
                                   ; Retry
                       86400
                                   ; Expire
                      2419200
                      604800 ) ; Negative Cache TTL
;
       NS
           nsl.tdeig.ch.
;*
              129.194.184.80
      Α
             A 129.194.184.80
;tdeig.ch.
    А
             129.194.184.84
ns1
WWW
       А
              129.194.184.80
ftp
      А
              129.194.184.80
secure A
              129.194.184.81
          129.194.184.89
ca A
lb
       А
              129.194.184.92
lb
       А
              129.194.184.93
lb
       А
              129.194.184.94
```

Redémarrer le service bind9 /etc/init.d/bind9 restart

### 8 Configuration du firewall Clavister

Il a fallu ajouter des règles sur le firewall du labo pour permettre de communiquer avec la nouvelle CA

Aller sur le Manager, puis créer un nouveau *Host* sous *Hosts* & *Networks*, que j'ai nommé CA\_WinServer2008. Ce *Host* désigne son adresse IP 129.194.184.89

Image: Security Editor       Image: Security Editor       Image: Security Editor         Image: Security Editor       Image: Security Editor       Image: Security Editor         Image: Security Editor       Image: Security Editor       Image: Security Editor         Image: Security Editor       Image: Security Editor       Image: Security Editor         Image: Security Editor       Image: Security Editor       Image: Security Gateways         Image: Security Editor       Image: Security Gateways       Image: Security Gateways         Image: Security Editor       Image: Security Gateways       Image: Security Gateways         Image: Security Gateways       Image: Security Gateways       Image: Security Gateways         Image: Security Gateways       Image: Security Gateways       Image: Security Gateways         Image: Security Gateways       Image: Security Gateways       Image: Security Gateways         Image: Security Gateways       Image: Security Gateways       Image: Security Gateways         Image: Security Gateways       Image: Security Gateways       Image: Security Gateways         Image: Security Gateways       Image: Security Gateways       Image: Security Gateways         Image: Security Gateways       Image: Security Gateways       Image: Security Gateways         Image: Security Gateways       Image: Security Gateways       Image: Security Gatew	🕂 File Edit Vier	w Action Tools Window Help			
Tools       Global Namespace       Name       Network         Application Layer Gateways       Application Layer Gateways       10.2.2.22         Security Editor       Certificates       10.2.2.22         Certificates       Certificates       10.2.2.22         User Databases       Certificates       10.2.2.22         User Databases       Certificates       10.2.2.22         VPN Settings       Certificates       10.1.1.3         Security Gateways       Certificates       10.1.1.10         Security Gateways       Certificates       11.1.10         Security Gateways       Certificates       10.1.1.10         Security Gateways       Certificates       10.1.1.10         Security Gateways       Certificates       10.1.1.5         Security Gateways       Certificates       10.1.1.5         Security Gateways       Certificates       10.1.1.5         Security Gateways       Colol Objects       Certailyst_C         Security Gateways       Color Objects       Certailyst_C	🗅 📽 🖬   X	• • • • • • • • • • • • • • • • • • •	<mark>6</mark> ₿D	eploy Configuration 👩 🖯 😗	₽    च= = + = + = = = = =
Image: Security Editor       Image: Security Editor         Image: Security Edit	Tools	🖃 🗠 🂁 Global Namespace		Name	Network
Application Layer Gateways       17       P BigBrother_New       10.1.1.3         Security Editor       Cartificates       18       E BigBrother_New       129.194.184.200         Security Editor       User Databases       19       P antivirus.unige.ch_New       10.194.9.164         Logging       Schedule Profiles       19       P antivirus.unige.ch_New       10.194.9.164         Log Analyzer       VPN Settings       21       P DC1       10.1.1.10         Security Gateways       22       Routeur_Surber       10.1.2.29         Security Gateways       23       Nagios       10.1.1.5         P Real-time Monitor       P Dis Authentication       25       DNS_Publique_tdeig.ch       129.194.184.89         Reseaux       26       C A_WinServer2008       129.194.184.89       26       27       Admin N New		Hosts & Networks	16	📮 Manager_New	10.2.2.22
Security Editor       Image: Certificates       18       BlueCoat_New       129.194.184.200         Schedule Profiles       Image: Certificates       19       Image: Certificates       19       Image: Certificates         Image: Certificates       Image: Certificates       19       Image: Certificates       10       Image: Certificates       19       Image: Certificates       19       Image: Certificates       10       Image: Certificates       10       Image: Certificates       19       Image: Certificates       10       Image: Certificates       11       Image: Certificates       11       Image: Certificates       11       Image: Certificates       11       Image: Certificates       12       Image: Certificates       11       Image: Certificates       11       Image: Certificates       11       Image: Certificates       11       Image: Certificates       12       Image: Certificates       12       Image: Certificates       12       Image: Certificates	7.	Services	17	📮 BigBrother_New	10.1.1.3
Security Editor       Image: Schedule Profiles       19       Image: antivirus.unige.ch_New       10.194.9.164         Image: Comparison of the schedule profiles       Image: Comparison of the schedule profiles       10       Image: Comparison of the schedule profiles         Image: Comparison of the schedule profiles       Image: Comparison of the schedule profiles       10       Image: Comparison of the schedule profiles         Image: Comparison of the schedule profiles       Image: Comparison of the schedule profiles       10       Image: Comparison of the schedule profiles         Image: Comparison of the schedule profiles       Image: Comparison of the schedule profiles       10       Image: Comparison of the schedule profiles         Image: Comparison of the schedule profiles       Image: Comparison of the schedule profiles       10       Image: Comparison of the schedule profiles         Image: Comparison of the schedule profiles       Image: Comparison of the schedule profiles       10       Image: Comparison of the schedule profiles         Image: Comparison of the schedule profiles       Image: Comparison of the schedule profiles       10       Image: Comparison of the schedule profiles         Image: Comparison of the schedule profiles       Image: Comparison of the schedule profiles       10       10       10         Image: Comparison of the schedule profiles       Image: Comparison of the schedule profiles       10       10       10 <t< th=""><th>34</th><th>Certificates</th><th>18</th><th>📮 BlueCoat_New</th><th>129.194.184.200</th></t<>	34	Certificates	18	📮 BlueCoat_New	129.194.184.200
Cog Analyzer         20 - xml.shavlik.com_New         216.182.4.8           Log Analyzer         VPN Settings         21 - DC1         10.1.1.10           Security Gateways         22 - Routeur_Surber         10.1.2.29           Real-time Monitor         Routing         24 - Catalyst_C         129.194.184.88           P - Local Objects         25 - DNS_Publique_tdeig.ch         129.194.184.89           P - Traffic Management         Réseaux         26 - CA_WinServer2008         129.194.184.89           P - User Authentication         27 - MAmin N New         10.2.0.0/16	Security Editor	Schedule Profiles	19	📮 antivirus.unige.ch_New	10.194.9.164
Cog Analyzer         VPN Settings         21         © DC1         10.1.1.10           Security Gateways         Security Gateways         22         © Routeur_Surber         10.1.2.29           Image: Security Gateways         Image: Security Gateways         23         © Nagios         10.1.1.5           Image: Security Gateways         Image: Security Gateways         23         © Nagios         10.1.1.5           Image: Security Gateways         Image: Security Gateways         24         © Catalyst_C         129.194.184.88           Image: Security Gateways         Image: Security Gateways         25         © DNS_Publique_tdeig.ch         129.194.184.89           Image: Security Gateways         Image: Security Gateways         26         © CA_WinServer2008         129.194.184.89           Image: Security Gateways         Image: Security Gateways         Image: Security Gateways         Image: Security Gateways           Image: Security Gateways         Image: Security Gateways         Image: Security Gateways         Image: Security Gateways           Image: Security Gateways         Image: Security Gateways         Image: Security Gateways         Image: Security Gateways           Image: Security Gateways         Image: Security Gateways         Image: Security Gateways         Image: Security Gateways           Image: Security Gateways			20	📮 xml.shavlik.com_New	216.182.4.8
Log Analyzer       Security Gateways       22       Routeur_Surber       10.1.2.29         Image: Security Gateways       Image: Security Gateways       23       Nagios       10.1.1.5         Image: Security Gateways       Image: Security Gateways       23       Nagios       10.1.1.5         Image: Security Gateways       Image: Security Gateways       24       Image: Catalyst_C       129.194.184.88         Image: Security Gateways       Image: Security Gateways       25       Image: DNS_Publique_tdeig.ch       129.194.184.89         Image: Security Gateways       Image: Security Gateways       26       Image: Catalyst_C       129.194.184.89         Image: Security Gateways         Image: Security Gateways       Image: Security Gateways       Image: Security Gateways       Image: Security Gateways       Image: Security Gateways         Image: Security Gateways       Image: Security Gateways       Image: Security Gateways       Image: Security Gateways       Image: Security Gateways       Image: Security Gateways         Image: Security Gateways       Image: Security Gateways       Image: Security Gateways       Image: Security Gateways       Image: Security Gateways         Image: Security Gateways       Image: Security Gateways	$\mathbf{Q}$	VPN Settings	21	📮 DC1	10.1.1.10
Log Analyzer         Prevaluzuolo         23         Nagios         10.1.1.5           Table         Routing         24         Catalyst_C         129.194.184.88           Decal-time Monitor         Decal Objects         25         DNS_Publique_tdeig.ch         129.194.184.89           Real-time Monitor         Decal Objects         26         CALWinServer2008         129.194.184.89           Research         Research         Research         Research         Research           Decal Objects         27         Admin N New         10.2.0.0/16	Log Appluger	🖻	22	Routeur_Surber	10.1.2.29
B         Interfaces         24         Catalyst_C         129.194.184.88           B         Interfaces         25         DNS_Publique_tdeig.ch         129.194.184.84           B         Local Objects         26         CA_WinServer2008         129.194.184.89           B         User Authentication         26         CA_WinServer2008         129.194.184.89           DUser Authentication         27         Admin N New         10.20.0/16	Log Analyzer		23	P Nagios	10.1.1.5
B     Interfaces       B     Local Objects       B     Local Objects       B     Local Objects       C     E       C <th>( - )</th> <th>E Routing</th> <th>24</th> <th>Catalyst_C</th> <th>129.194.184.88</th>	( - )	E Routing	24	Catalyst_C	129.194.184.88
Real-time Monitor         Image: Construction         26         E CA_WinServer2008         129.194.184.89           Image: Construction         Image: Construction         Réseaux         Image: Construction         Image		⊡ Interfaces     □ Local Objects	25	DNS_Publique_tdeig.ch	129.194.184.84
Construction     C	Real-time Monitor		26	CA_WinServer2008	129.194.184.89
Dervice Powerking 27 Admin N New 10.2.0.0/16		🕀 🖳 Traffic Management		Réseaux	
			27	😼 Admin_N_New	10.2.0.0/16
B → Miscellaneous     28 및 Ext_N_New     129.194.184.0/22		🗄 Miscellaneous	28	💼 Ext_N_New	129.194.184.0/22
Remote Console 🗄 — Advanced Settings 29 🗒 Int. N_New 10.1.0.0/16	Remote Console	it in Advanced Settings	29	a Int_N_New	10.1.0.0/16
30 🕎 pptp_pool 10.1.2.230 - 10.1.2.239	<u> </u>		30	😼 pptp_pool	10.1.2.230 - 10.1.2.239
31 🗒  2tp_pool 10.1.2.249			31	📲 l2tp_pool	10.1.2.240 - 10.1.2.249
Bealtime Log 32 2 DMZ_N_New 129.194.184.0/22	Real-time Log		32	B DMZ_N_New	129.194.184.0/22
33 🕎 EIVD_N 10.4.0.0/16			33	😼 EIVD_N	10.4.0.0/16
34 🕎 Adsl_N 10.3.0.0/16	~		34	📲 Adsl_N	10.3.0.0/16
35 🗒 Zero_N 0.0.0.0/8	1		35	🗐 Zero_N	0.0.0.0/8
Licenses 36 🕎 LocalHost_N 127.0.0.0/8	Licenses		36	📲 LocalHost_N	127.0.0.0/8
37 🗒 Multicast_N 224.0.0.0/3			37	🗐 Multicast_N	224.0.0.0/3
38 🕎 Surber_N 10.100.0.0/16			38	💼 Surber_N	10.100.0.0/16
39 🖉 All_N_New 0.0.0.0/0			39	All_N_New	0.0.0.0/0
Groupes de réseaux ou de machines				Groupes de réseaux ou de m	achines
40 🕎 Dmz_Servers_New SSL_CA_Publique, DNS_Publique, Web_Publique, DNS_Publique_tdeig.			40	🖫 Dmz_Servers_New	SSL_CA_Publique, DNS_Publique, Web_Publique, DNS_Publique_tdeig.ch, C

On va aussi ajouter notre Host au groupe de serveurs DMZ (des règles sont créées pour ce groupe, afin d'autoriser le ping par exemple)

Global	Namespace : Host & N	etwork Properties - 40	) (Dmz_Ser 🗵					
Hosts & Networks User Authentication Usage								
Use a Hosts & Networks item to define a name for a specific IP network.								
Ger	General							
1	Name: Dmz_Servers_New							
	Lype: O Host	O Network O Bange	C Group					
<u>S</u> pe	ecification							
	Name	Range	Exclui 📥					
	💂 SSL_CA_Publique	129.194.184.81						
	💂 DNS_Publique	129.194.184.212						
	💂 Web_Publique	129.194.184.80						
	💂 DNS_Publique_tdei	129.194.184.84						
	🚆 CA_WinServer2008	129.194.184.89	-					
	•							
	<b>↑</b> ↓	Exclude	$+ \times$					
Cor	nments							
1	↓ ↓		Close					

oclavister Fine 1 🌐	une - [Security Editor - Data Source: 'Firewall_L	abo']					<u>_8×</u>
🤠 File Edit View	v Action Tools Window Help						_ 8 ×
0 📽 🖬   🐰	h 🗈 🔲 🖻 👆 🖬 🦌 🖌 🖌	😚 Deploy Configuration 😚 👩	Ì║┱╴ <sub>╋╴</sub> ╋╴┓	±   🗎	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1		
Tools	🖃 🚭 Global Namespace	Name	Action	Log	Source Interface	Source Network	Destination 🔺
	Hosts & Networks	11 🐺 AllowPingFromInt	🚻 Allow		🖳 Int_I	👼 Int_N_New	🖳 any
3.1	Services	12 🐺 IntToAll-FtpActif	🚻 NAT		💵 Int_I	📜 Int_N_New	💵 any
130	Certificates	13 🐺 IntToAll	III NAT		Int_I	🗐 Int_N_New	🔊 any
Security Editor	Schedule Profiles	Accès au Serveurs Publiques					
0	User Databases	14 🐺 PingLabo	Allow		💵 any	Ext_N_New	🕎 Dmz_I
Q	VPN Settings	15 🐺 Web	Allow		🖳 any	All_N_New	B Dmz_I
Las Australia	🖻 🔄 Security Gateways	16 🐺 RnisSite	Allow		B any	All N New	Dmz I
Log Analyzer		17 3 Dns	Allow		B any	All N New	B Dmz I
00	E Couting	18 3 55L-CA	711 Allow		III) anv	All N New	Dmz I
SP		19 JE BlueCoat	70 Allow		B any		Dmz I
Beal-time Monitor		20 BlueCoatHttps	TI Allow		B any		Dmz I
	🕂 📄 Traffic Management	21 Ftp			B) any		
	🗄 🖳 User Authentication	22 S DNS Ideia ch			BD any		
		22 SSL CA WinServer2008			III) any		
Remote Console	🗄 🧰 Advanced Settings	Dm2 vers Externe	HIOW		-gr any		
A		24 SpropállToInt	Drop		B) any	All N New	BB any
Que		2F B DMZSeruproToInternet	TT Allow		The second secon		
		25 The Division of the deba				Dinz_Servers_New	
Heal-time Log		20 B Dinzbervermickreeopuale				Dhiz_bervers_New	
					mm Dmz_1		Gw_Grc
						P Directat_New	Gw_Grc
Licenses		29 St DmzServerNTP	Allow TTD		By Dmz_1	Servers_New	GW_Grc
		3U STOrV19			Drnz_1	DNS_Publique	Gw_Grc
		31 VE FWNTP	Allow		∎ <b>y</b> any	Ext_H_New	■∰ any
		32 😻 FtpActif	Allow		Dmz_I	Veb_Publique	any any
		33 🕸 DNSfor_tdeig.ch	Allow		Drnz_I	💂 DNS_Publique_tdeig.ch	🗊 Gw_Grc
		LastRule			Lana		Lana I
		34 🐺 DropAll	💷 Drop		🖳 any	All_N_New	🖳 any
	J	•					•
Ready		1					NUM
🏄 Start 🔀 🥭	🖸 🖾 🛛 🏥 🔯 Clavister FineTune - [	led - Paint				1	ይ 💟 💁 11:17
Firewall200	6 : Rule Properties - 23 (SSL_CA	WinServer2008)			×		
Rule	ervice   Schedule   Log Settings   Ar	ddress Translation					
					1		

# Puis créer une nouvelle règle afin d'autoriser le flux http vers notre CA

A rule item specifies what action to perform on network traffic that matches the specified filter criteria.  General <u>Name:</u> SSL_CA_WinServer2008	
General	
Name: SSL_CA_WinServer2008	
Action:	
Address Filter	
Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.	•
Source Destination	
Interface: 💷 any 💌 🛄 Dmz_I 💌	
N <u>e</u> twork: All_N_New	
Comments	
	use

Sous l'onglet Service ci-dessus, sélectionner http-in-all

Clavister FineT	une - [Security Editor - Data Source: 'Firewall_L	abo']					
		29 Deploy Configura	ation 者 8 👷 8	#F 3+ 3+ 3.   ₽ 3+			크먹스
Tools			Interface	Network	Gateway	Local IP	Proxy AR
T OOIS	Hosts & Networks	1 - P Route	Internet	Re Surber N	B Routeur Sur	Local I	11000 110
NON	Application Layer Gateways	2 - Route	B Admin I	E Admin N New			
1 ac	Certificates	3 - Route	Int I	E Int N New			
Security Editor		4 - Route	Dmz I	S Web Publique			Ext I
	🗄 User Databases	5 J Boute	Dmz I	DNS Publique			Ext I
Q	Europy Logging	6 Proute		DNS Publique Ideia.cb			Evt I
	E-Security Gateways	7 - P Route		SSL CA Publique			Evt I
Log Analyzer	Firewall2006	8 C Poute		CA WipServer2008			Evt I
0		9 C Poute		Cataluct C			Evt I
SP .	Routes الم	10 - P Route		BlueCoat New			Evt I
Beal-time Monitor	Policy-Based Routing Tables	11 P Route					Dmz I
Thear time informed	DHCP Relay	12 P Route					
	H Multicast	13 P Poute			Cui EIC New		
	OSPE	10 - Route					
Remote Console		14 - Rouce	Mgr Adsi_1	W AII_N_NEW	E Gw_HOSI		
	🗈 🖳 Local Objects						
Ready		*					
🛃 Start 🔀 🎒	🔄 🔤 🛛 🤠 Clavister FineTune - [ 🦉 clavi	ster1-1.bmp - Paint				۲	💟 💽 11:19
Firewall2006	- Poute Properties - 8	×	Eirowall2	006 · Doute Properties	. 9		×I
(Davis) p	upplues l	_		Down ADD in the last	- 0		
	oxy ARP   Monitor	1	Route	Proxy ARP Monitor			1
	A route item defines what interface and	gateway to	Proxy /	\RP			
- <b>-</b>	use in order to reach a specified networl	с.	LISE	Proxy ABP to dynamically	nublish ABP items f	or this	
General			rou	e on the specified interface	s.		
General -							
Interfac	e: 💷 Dmz I			RP Name Additi	onal information		
				🗒 Admin_I Admir	_H_New		
<u>N</u> etwor	k: 🖪 CA_WinServer2008			🗒 Int_I Int_H	_New		
	) <b>e</b>			🗒 Ext_l Ext_H	LNew		
<u>G</u> atewa	ay:	$\overline{}$		🖽 Dmz_I DMZ_	H_New		
	J			🕎 Adsl_I Adsl_I	Н		
<u>L</u> ocal II	P Address:			📆 Gw_Gro Ext_l,	Adsl_l		
	J					_	
<u>M</u> etric:						<u>~</u>	
<u>C</u> omments				<u>S</u> elect All <u>C</u> lear All			
				Always salast ALL interfere	a including now -	200	
				Mways select ALL Intellace	es, moluung new of	108	
	1			• 1		~	1
<b>T</b> +		Llose		<b>↓</b>		Llose	1

# Puis, il faut créer une nouvelle route afin d'activer le routage vers notre CA :

Il ne reste plus qu'à uploader la nouvelle config sur le firewall !