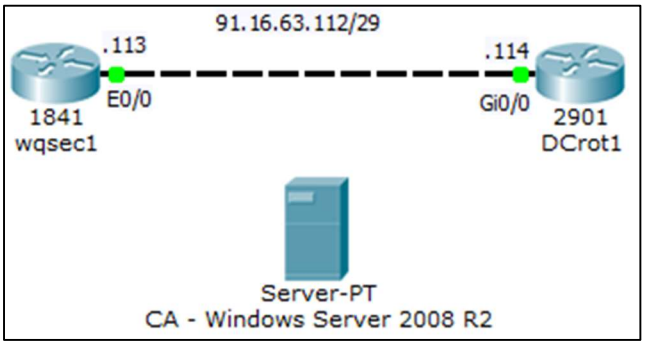
IPSec entre Cisco Asa e Cisco Router – Certificado Assinado por CA em Cisco Router

Neste procedimento será demostrada como configurar configurar um túnel IPSec entre um ASA e um Roteador usando certificados assinados por uma CA Windows. Para a realização deste procedimento foi utilizada a topologia abaixo:



Equipamentos utilizados:

- **CA:** Windows Server 2008 R2
- **wqsec1:** Cisco ASA 5505 com Software 8.2(5)
- **DCrot1:** Cisco Router 2901 com IOS 15.1(4)M4

Todo o tráfego entre o "**wqsec1**" e "**DCrot1**" será criptografado através do túnel IPSec. Para criptografia será usado o "**AES256**" e para integridade o "**SHA**".

Quando utiliza-se certificados para autenticação, é extremamente necessário que o relógio dos equipamentos esteja sincronizado. Verifique o horário em todos os equipamentos antes de efetuar os procedimentos abaixo.

Este procedimento se divide em quatro partes:

- Configuração de endereçamento e comunicação entre os equipamentos
- Configuração dos certificados
- Configuração do IPSec
- Verificação

Para configurar os equipamentos siga os passos abaixo:

Configuração de endereçamento e comunicação entre os equipamentos

wqsec1

1. Configure o nome de Host do equipamento com o comando abaixo:

```
ciscoasa(config)# hostname wqsec1
```

2. No ASA 5505, não é possível configurar o endereçamento na interface física. Para configurar o endereçamento é necessário criar uma interface VLAN, configurar o endereçamento IP na mesma, identifica-la com um nome (caso o nome seja "**inside**" a interface será configurada com o nível de segurança "**100**", mas se for "**outside**" será configurado com o nível de segurança "**0**", automaticamente) e vincular a interface física à VLAN. Nos comandos abaixo é configurado o endereçamento no equipamento:

```
a. wqsec1(config)# interface vlan 1
b. wqsec1(config-if)# ip address 91.16.63.113 255.255.255.248
   wqsec1(config-if)# no shutdown
c. wqsec1(config-if)# nameif outside
   INFO: Security level for "outside" set to 0 by default.
   wqsec1(config-if)# exit

d. wqsec1(config)# interface ethernet 0/0
e. wqsec1(config-if)# switchport access vlan 1
   wqsec1(config-if)# no shutdown
   wqsec1(config-if)# exit
```

a. Cria a "**VLAN 1**" e acessa a interface "**VLAN 1**"
b. Configura o endereçamento na interface "**VLAN 1**"
c. Identifica a interface como "**outside**"
d. Acessa a interface "**Ethernet 0/0**"
e. Ingressa a interface na "**VLAN 1**"

DCrot1

1. O comando abaixo configura o nome de Host do equipamento.

```
Router(config)#hostname DCrot1
```

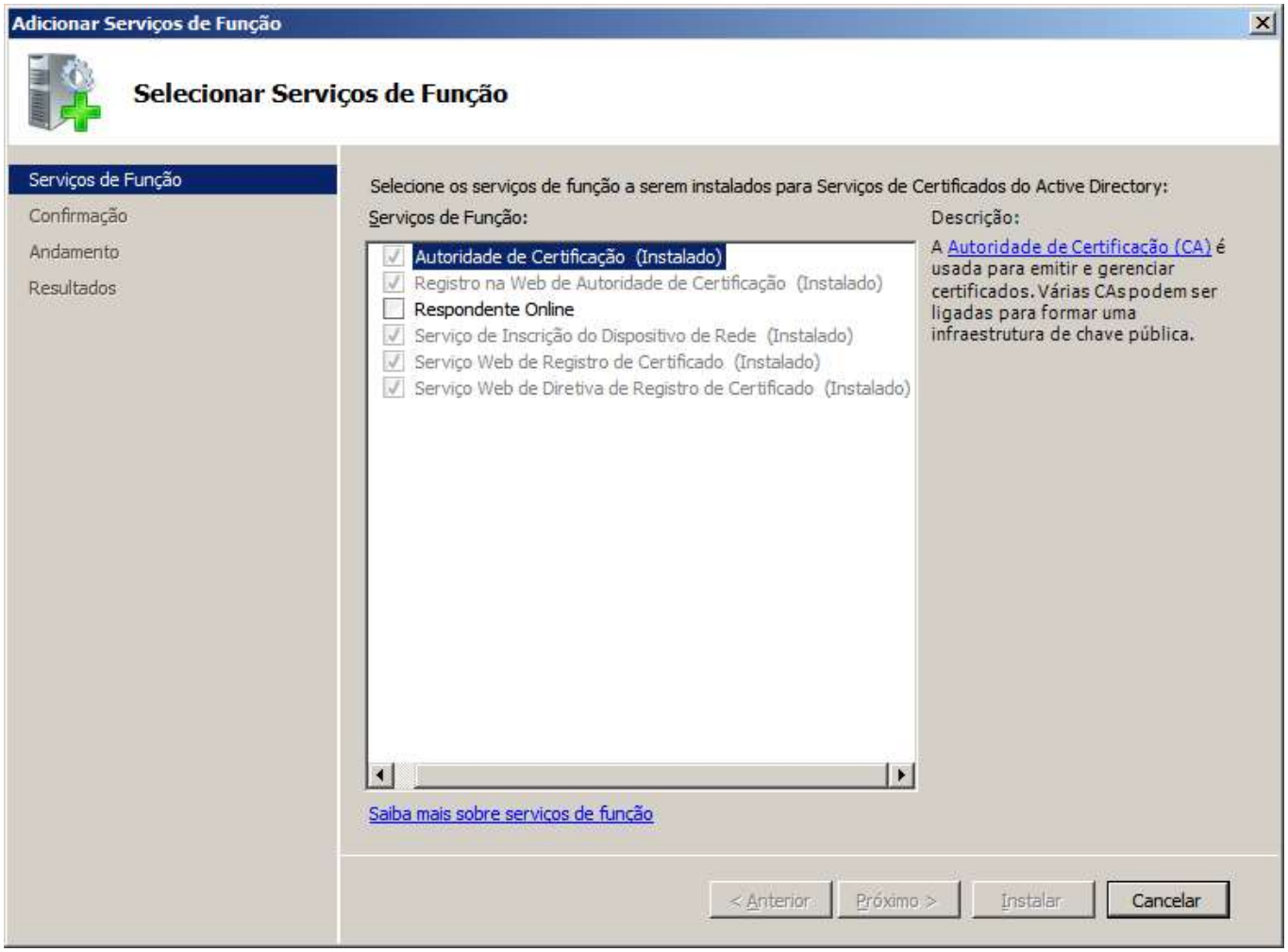
2. Os comandos abaixo configuram o endereçamento na interface "**GigabitEthernet 0/0**" do equipamento.

```
DCrot1(config)#interface gigabitEthernet 0/0
DCrot1(config-if)#ip address 91.16.63.114 255.255.255.248
DCrot1(config-if)#no shutdown
DCrot1(config-if)#exit
```

Configuração dos certificados

CA

1. Para emitir certificados utilizando uma CA Windows é necessários que a função "**Serviços de Certificados do Active Directory**" e os serviços de função estejam instalados conforme imagem abaixo.



wqsec1

1. O comando abaixo ajusta o horário do equipamento

```
wqsec1# clock set 14:47:00 03 JUN 2014

wqsec1# show clock
14:47:05.169 UTC Tue Jun 3 2014
```

2. O comando abaixo configura o domínio "**pesquisa.local**" no equipamento.

```
wqsec1(config)# domain-name pesquisa. local
```

3. O comando abaixo remove todas as chaves privadas do equipamento.

```
wqsec1(config)# crypto key zeroize rsa
```

4. O comando abaixo cria uma chave privada com o nome "**private.key**" com o tamanho do módulo "**1024**".

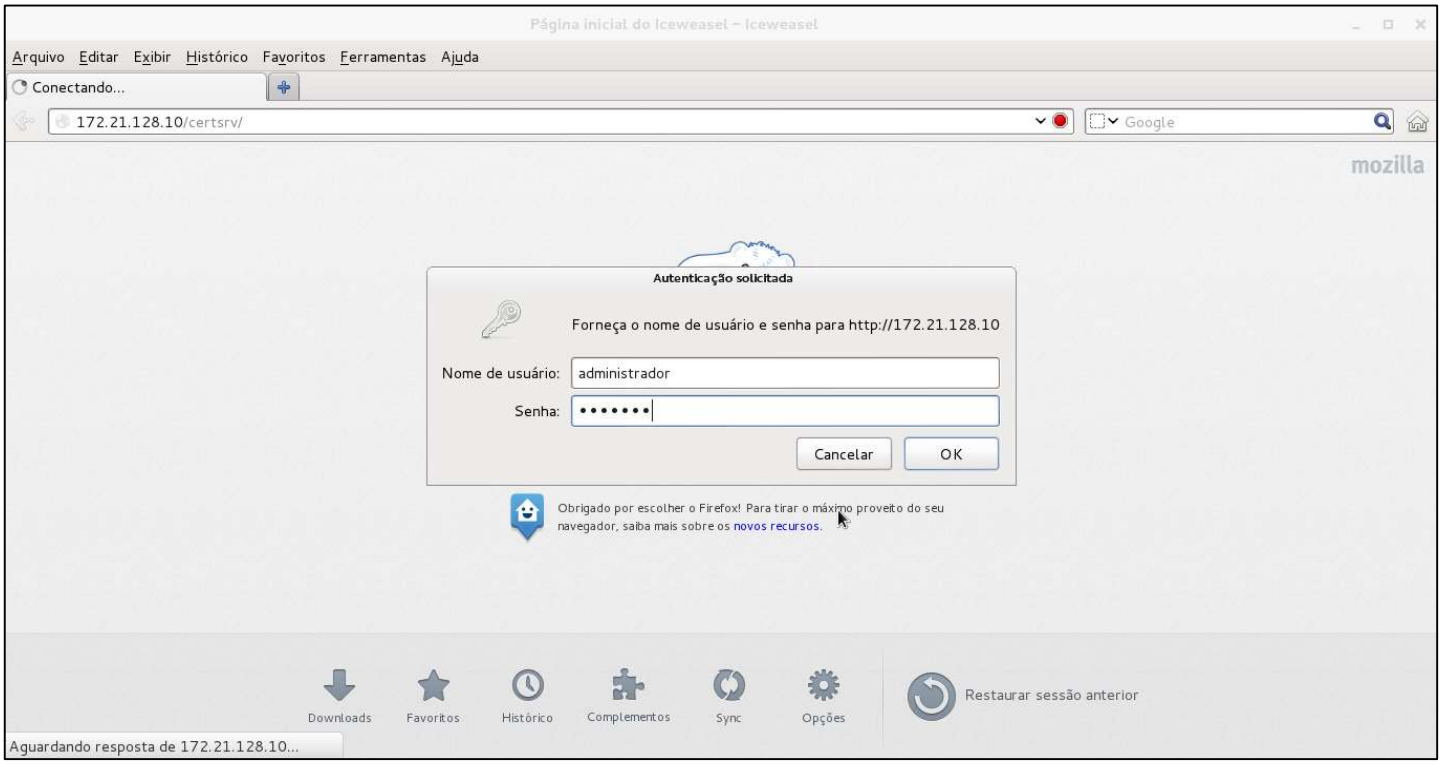
```
wqsec1(config)# crypto key generate rsa label private.key modulus 1024
```

5. Os comandos abaixo configuram um trustpoint com o nome "**CA**".

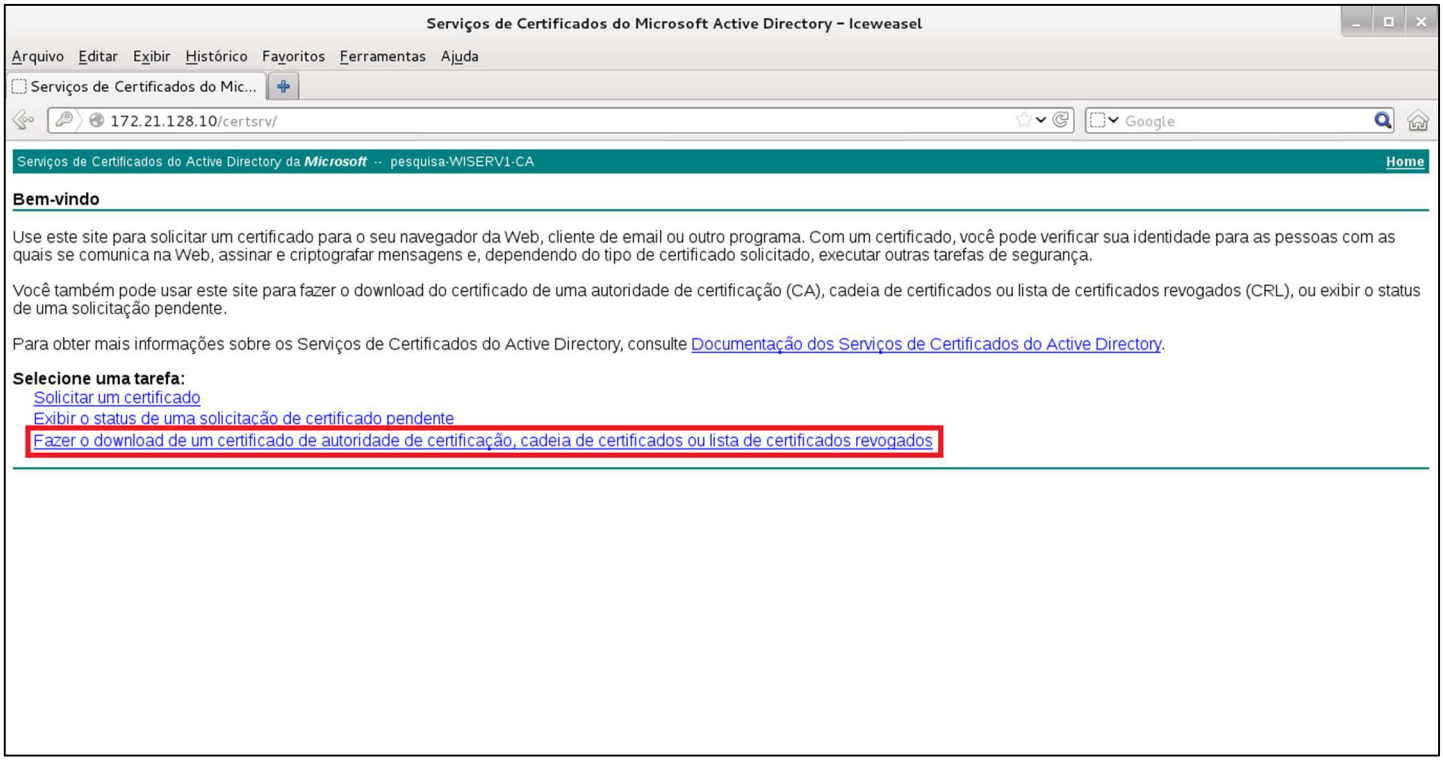
```
a. wqsec1(config)# crypto ca trustpoint CA
b. wqsec1(config-ca-trustpoint)# enrollment terminal
c. wqsec1(config-ca-trustpoint)# fqdn wqsec1.pesquisa.local
d. wqsec1(config-ca-trustpoint)# subject-name CN=wqsec1.pesquisa.local
e. wqsec1(config-ca-trustpoint)# keypair private.key
f. wqsec1(config-ca-trustpoint)# ignore-ipsec-keyusage
   wqsec1(config-ca-trustpoint)# exit
```

a. Cria um trustpoint com o nome "**CA**".
b. Configura o método de inscrição via terminal (cut-and-paste)
c. Configura o nome de domínio totalmente qualificado como "**wqsec1.pesquisa.local**".
d. Configura o subject-name do trustpoint como "**CN=wqsec1.pesquisa.local**".
e. Especifica o nome da chave gerada anteriormente para esta identidade.
f. Configura para suprimir o uso da chave verificando certificados de cliente IPSec

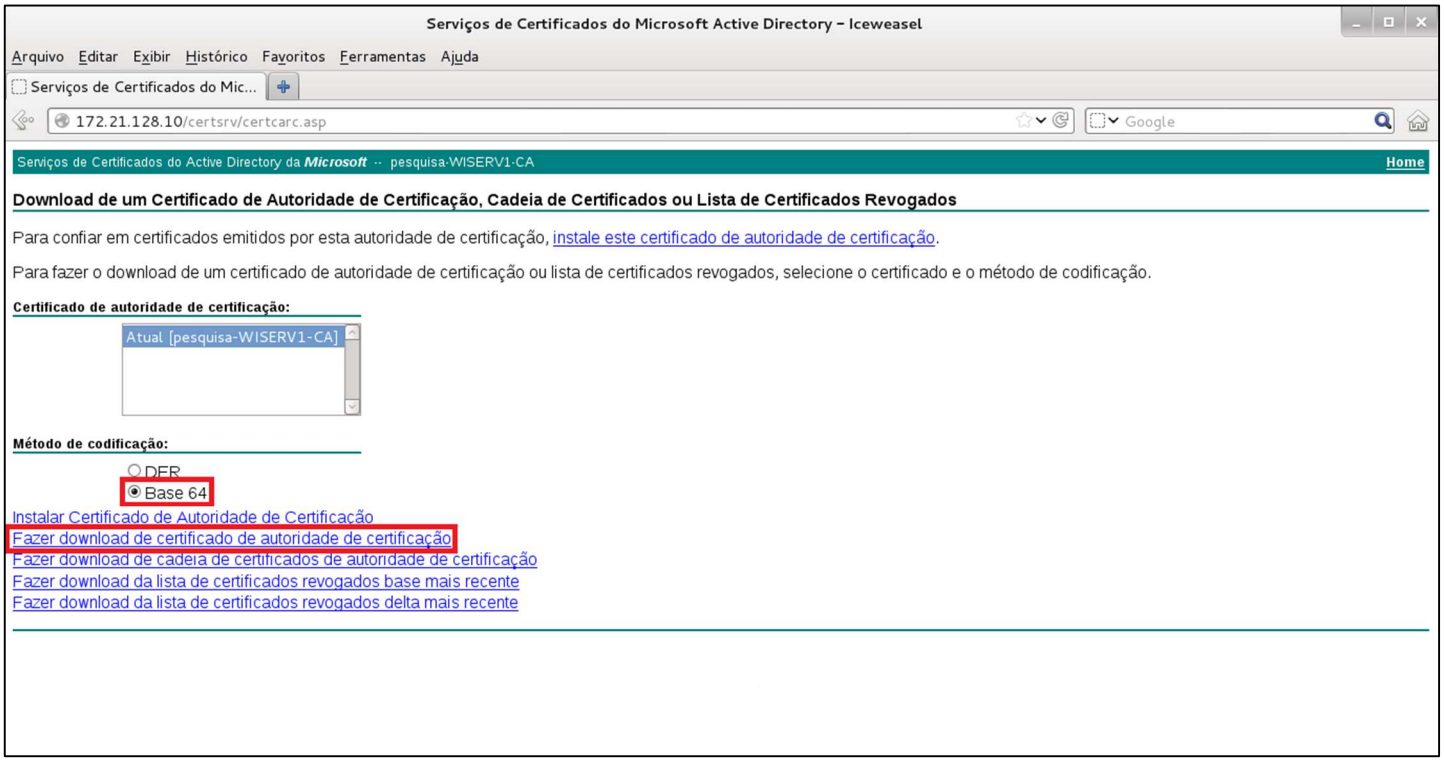
6. Para obter o certificado da CA, em um navegador acesse a URL "**http://ip-do-servidor/certsrv**". Insira o usuário e senha e clique em "**OK**".



7. Clique em "**Fazer o download de um certificado de autoridade de certificação ...**"



8. Selecione o método de certificação “**Base 64**” e clique em “**Fazer download de certificado de autoridade de certificação**”.



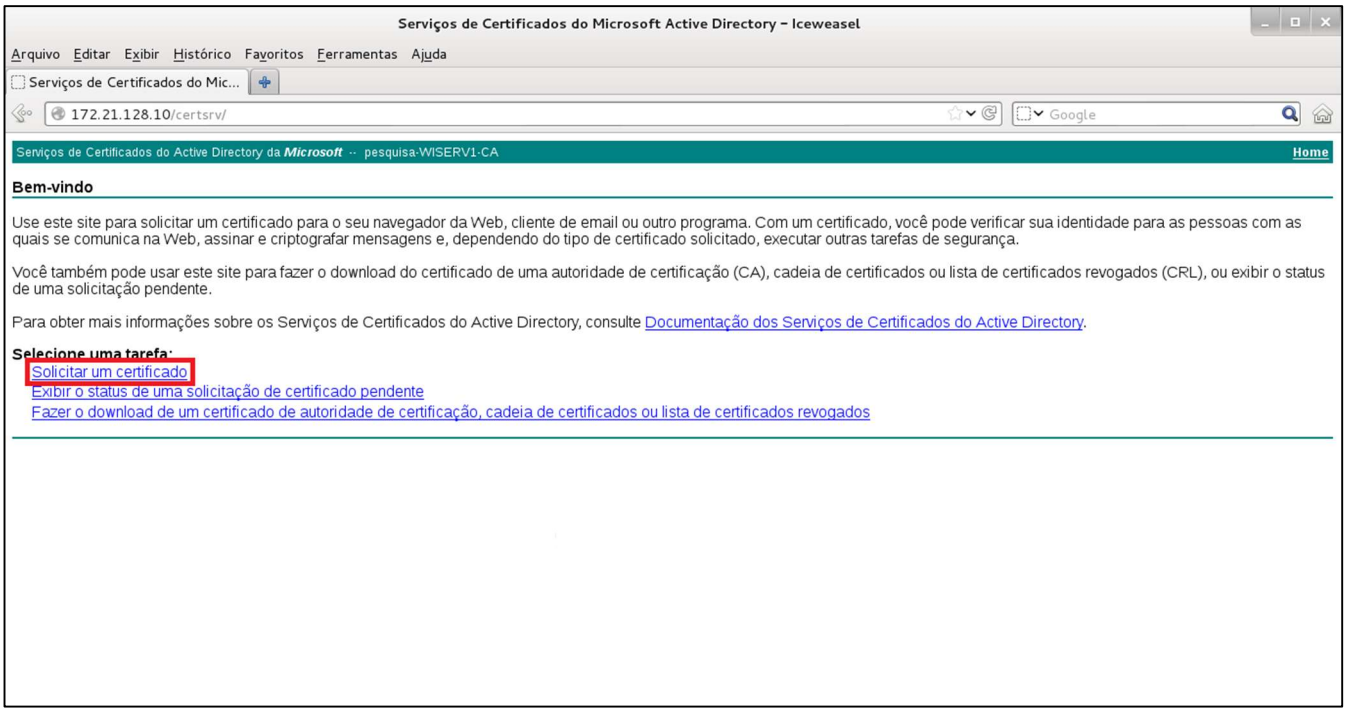
9. Insira o comando abaixo para importar o certificado da CA. Abra o arquivo de certificado da CA, copie o conteúdo e cole no terminal. Após colar o conteúdo do certificado, pressione "**Enter**", digite "**quit**" e pressione "**Enter**" novamente.

```
wqsec1(config)# crypto ca authenticate CA
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIDeTCCAmGgAwIBAgIQYmyPMBK3g5VJE2/hfPEivTANBgkqhkiG9w0BAQUFADBP
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghwZXNxdWlz
YTEcMBoGA1UEAxMTcGVzcXVpc2EtV0lTRVJWMS1DQTAeFw0xNDA1MDkxMTQwMzNa
Fw0xOTA1MDkxMTUwMzBaME8xFTATBgoJkiaJk/IsZAEZFgVsb2NhbDEYMBYGCgmS
JomT8ixkARkWCHBlc3F1aXNhMRwwGgYDVQQDExNwZXNxdWlzYS1XSVNFUlYxLUNB
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwm5nUFh+/9dGLMVJx8W+
sBnH17Zh6Nta07zwzxNoPwRth7lfqr75WqzEUY4lKXzz+XGEPYRsaLBwMEmJbZ+y
WizVCzWQ9Am3TAyw4kJXfiik2BYORsIQziM8GK4u50qzccLzWwAkAgzY/CElcngD
sPoGBo8N208ARcu+aky31pRM6qX96Popl87ftN2+tNkjeaNxah7iJlN5hkzu9CPX
MNemuwnjf5s3vDI+oNppcTSA3R6c451iOH9ZgYRso8NaCOsTHs2mbhcAEPkaP8xF
7OorZxmQq0ruSVDFn2MmuK0UzmFhoWHdM2MLGjkEDimYIGxMVb1MMMQmh1NF70nG
8QIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4E
FgQU46LJul+7sSUNX2Lu9Sl+mmyDAGgwEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZI
hvcNAQEFBQADggEBABbo22mWVeT3TQClauNBwKBaxw2EvOya5jnSpCkiKw4QYcPL
OfIe1zkwd0+/EFUysJwK6OeNawY8xxxHuEakTXXqjbEM8w5jXVUSo7rOLcTTM8rf
+EgelxQeSwgscLB+y774rMS9HissKjvu27+xbYRKh0GGZtwknKYiakQbisnQS4h8
HNCz9Nlnf3kv0ivpy7hxq4MTOBCyO8t7ThkMz8Z87YOGR1kptLM6JURZAKCusaTM
VulOcNSeaC8T7wkZFlgQpgbItHmI3vDHub0M8nzy8yNk/CNMLrAGnI9N6XYk7J9O
Zku3ouZNqiVgM2ngL2PzWp7RJ7raTOiN/EnW/R4=
-----END CERTIFICATE-----
quit

INFO: Certificate has the following attributes:
Fingerprint:    04f844eb b0a2d8bc a86e5543 05ac74ee
Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported
```

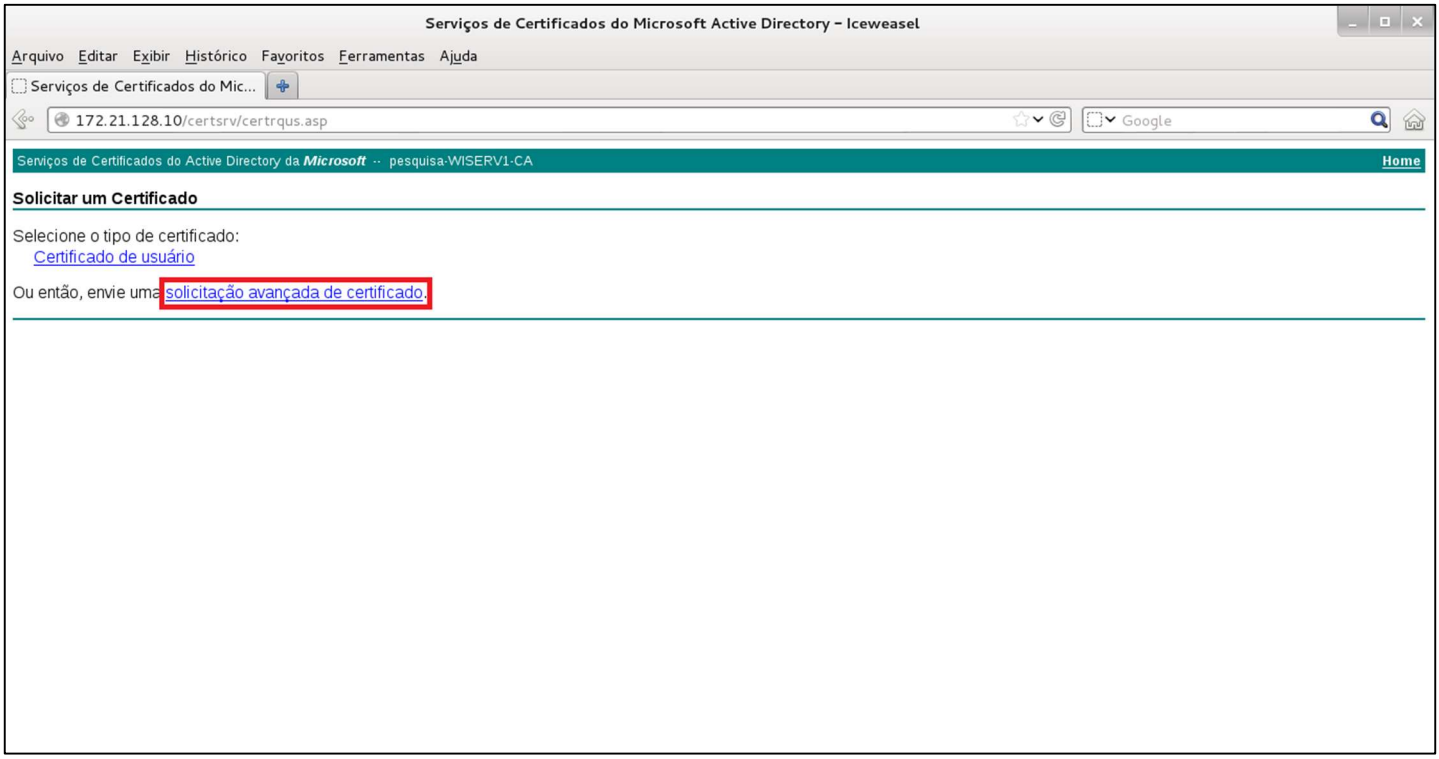
10. O comando abaixo gera uma requisição de certificado.

```
wqsec1(config)# crypto ca enroll CA
% Start certificate enrollment ..
% The subject name in the certificate will be: CN=wqsec1.pesquisa.local

% The fully-qualified domain name in the certificate will be: wqsec1.pesquisa.ll

% Include the device serial number in the subject name? [yes/no]: no

Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
-----BEGIN CERTIFICATE REQUEST-----
MIIByTCCATICAQAwRjEeMBwGA1UEAxMVd3FzZWMxLnBlc3F1aXNhLmxvY2FsMSQw
IgYJKoZIhvcNAQkCFhV3cXNlYzEucGVzcXVpc2EubG9jYWwwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAKgJdskYW7b4qehfvGz4M5/0d4wQq4Zhre7MK9qF4n/p
ZBdnyfA5fThx3khy61rauYRnCz5RB+d303PdgJ/rSTQbFQpr9kxcOXcjMCUI2lTS
ShipW8PUjcv6JWkroZsnKAuAun4ohi1xPZluw9ljlbI66aVg7IYnKbSBUr4BKu1p
AgMBAAGgQzBBBgkqhkiG9w0BCQ4xNDAyMA4GA1UdDwEB/wQEAwIFoDAgBgNVHREE
GTAXghV3cXNlYzEucGVzcXVpc2EubG9jYWwwDQYJKoZIhvcNAQEFBQADgYEAb3j5
1Ms8MLYunMrpA3cg+fYWdR1Xg1CHy4YHv60hzT9DiAT/UEKX94mcgKguUzAlDWPT
35uqfLnm5WUfS5zpPIW7KF11VdYTMCBAUUapPNi+c6W7181e3m2vQDq3MDD4B5p4
xlJWTlRZcyAXwKapHtd3+nX7EQKENhnUnPurjp8=
-----END CERTIFICATE REQUEST-----

Redisplay enrollment request? [yes/no]: no
```

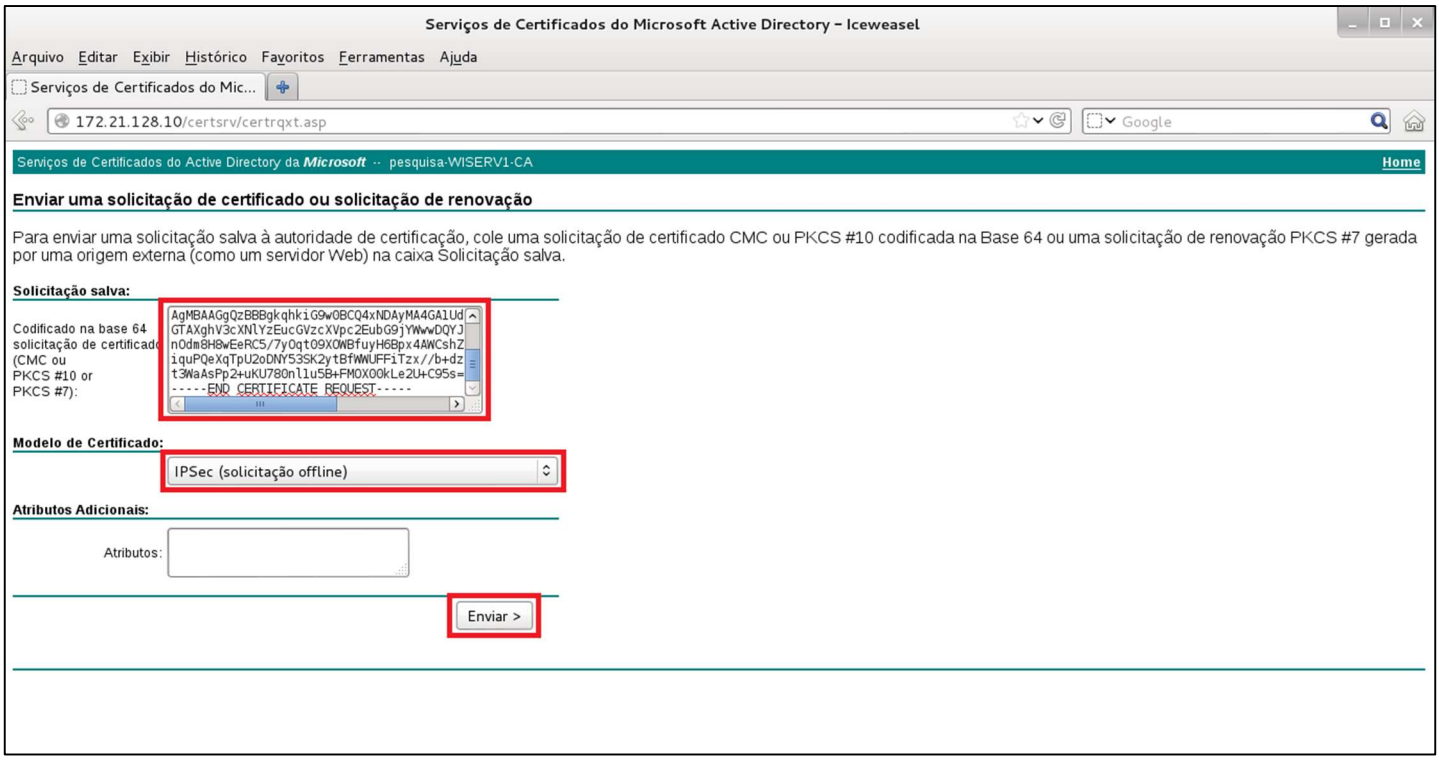
11. Na página principal da CA, clique em "**Solicitar um certificado**".



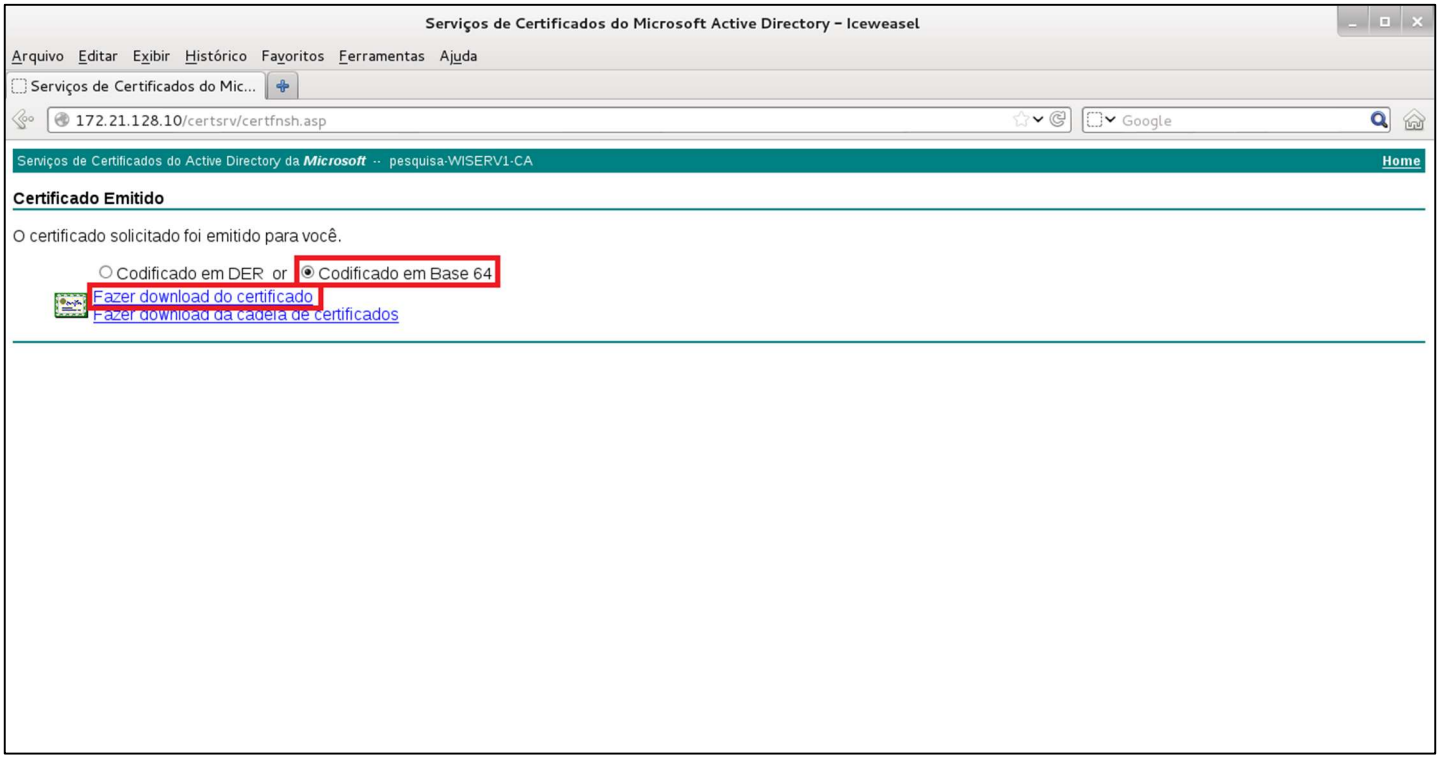
12. Clique em “**solicitação avançada de certificado**”.



13. Copie a requisição de certificado gerada no passo 10, cole no campo “**Certificado na base 64...**”, selecione o modelo “**IPSec (solicitação offline)**” e clique em “**Enviar**”.



14. Selecione “**Codificado em Base 64**” e clique em “**Fazer download do certificado**”.



15. Insira o comando abaixo para importar o certificado assinado pela CA. Copie o conteúdo do certificado obtido no passo 14 e cole no terminal. Após colar o conteúdo do certificado, pressione “**Enter**”, digite “**quit**” e pressione “**Enter**” novamente.

```
wqsec1(config)# crypto ca import CA certificate

% The fully-qualified domain name in the certificate will be: wqsec1.pesquisa.local


Enter the base 64 encoded certificate.
End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIFBTCCA+2gAwIBAgIKEU1QTgAAAAAASDANBgkqhkiG9w0BAQUFADBPMRUwEwYK
CZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghwZXNxdWlzYTEcMBoG
A1UEAxMTcGVzcXVpc2EtV0lTRVJWMS1DQTAeFw0xNDA2MDMxODQ4NDVaFw0xNjA2
AGUAcgBtAGUAZABpAGEAdABlAE8AZgBmAGwAaQBuAGUwEwYDVR0lBAwwCgYIKwYB
BQUIAgIwDQYJKoZIhvcNAQEFBQADggEBAElOpBaXrtc+kPYaQHh8UDH04JBm7Ypp
kEL6ADmSp08XmiUF86HGEJ8D4tZjqKg+1N6KqNh8QM823Ax8ki2+iGGMj0VwVy0a
yjcEaNNAoR0tXuYacof2KUqd3lRXOJs1qfui9o/l7hFTXshAVjVoDcvtRIygMo/d
aU/VWYT0hZsVPjTso0kwx+pU4e/U55hz+/QEDkyICj9So2AIUt39XuM2q0elZoGS
EXe6CyhNpFXv6EvsjueiPppSWD9yZMqtxowoku3jB5pY+M+iqP8IPnrNPxdD+IUd
lYuvm+pfT6Zv5QN7etECBL4B0RbZ6Oz3eUhf3vACDcyvhdlVxBpJl7s=
-----END CERTIFICATE-----
quit
INFO: Certificate successfully imported
```

DCrot1

1. O comando abaixo ajusta o horário do equipamento

```
DCrot1#clock set 16:07:25 03 JUN 2014

DCrot1#show clock
16:07:26.827 UTC Tue Jun 3 2014
```

2. O comando abaixo configura o domínio "**pesquisa.local**" no equipamento.

```
DCrot1(config)#ip domain-name pesquisa.local
```

3. O comando abaixo remove todas as chaves privadas do equipamento.

```
DCrot1(config)#crypto key zeroize rsa
```

4. O comando abaixo cria uma chave privada com o nome "**private.key**" com o tamanho do módulo "**1024**".

```
DCrot1(config)#crypto key generate rsa label private.key modulus 1024
```

5. Os comandos abaixo configuram um trustpoint com o nome "**CA**".

```
a. DCrot1(config)#crypto pki trustpoint CA
b. DCrot1(ca-trustpoint)#enrollment terminal
c. DCrot1(ca-trustpoint)#fqdn DCrot1.pesquisa.local
d. DCrot1(ca-trustpoint)#subject-name CN=DCrot1.pesquisa.local
e. DCrot1(ca-trustpoint)#revocation-check none
f. DCrot1(ca-trustpoint)#rsakeypair private.key
   DCrot1(ca-trustpoint)#exit
```

a. Cria um trustpoint com o nome "**CA**".
b. Configura o método de inscrição via terminal (cut-and-paste)
c. Configura o nome de domínio totalmente qualificado como "**DCrot1.pesquisa.local**".
d. Configura o subject-name do trustpoint como "**CN= DCrot1.pesquisa.local**".
e. Ignora a verificação de revogação.
f. Especifica o nome da chave gerada anteriormente para esta identidade.

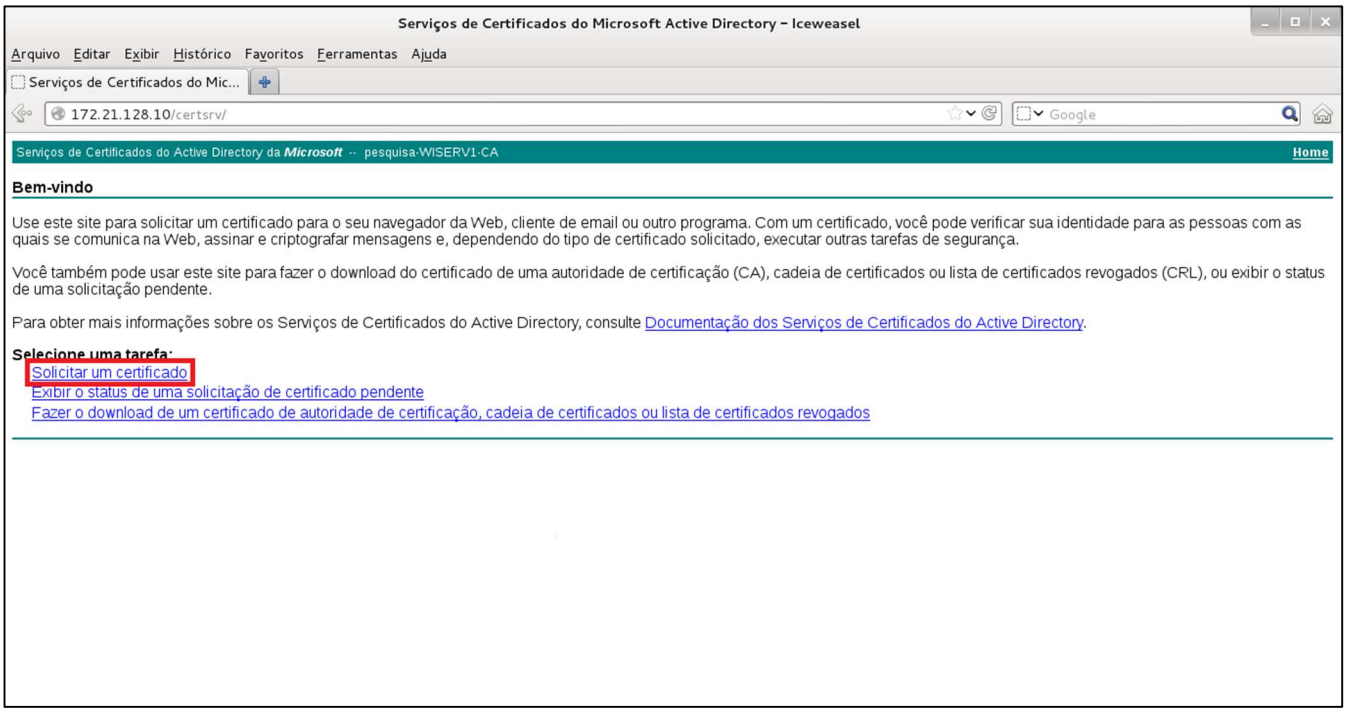
6. Insira o comando abaixo para importar o certificado da CA. Abra o arquivo de certificado da CA, copie o conteúdo e cole no terminal. Após colar o conteúdo do certificado, pressione "**Enter**", digite "**quit**" e pressione "**Enter**" novamente.

```
DCrot1(config)#crypto pki authenticate CA

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDeTCCAmGgAwIBAgIQYmyPMBK3g5VJE2/hfPEivTANBgkqhkiG9w0BAQUFADBP
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghwZXNxdWlz
YTEcMBoGA1UEAxMTcGVzcXVpc2EtV0lTRVJWMS1DQTAeFw0xNDA1MDkxMTQwMzNa
Fw0xOTA1MDkxMTUwMzBaME8xFTATBgoJkiaJk/IsZAEZFgVsb2NhbDEYMBYGCgmS
JomT8ixkARkWCHBlc3F1aXNhMRwwGgYDVQQDExNwZXNxdWlzYS1XSVNFUlYxLUNB
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwm5nUFh+/9dGLMVJx8W+
sBnH17Zh6Nta07zwzxNoPwRth7lfqr75WqzEUY4lKXzz+XGEPYRsaLBwMEmJbZ+y
WizVCzWQ9Am3TAyw4kJXfiik2BYORsIQziM8GK4u50qzccLzWwAkAgzY/CElcngD
sPoGBo8N208ARcu+aky31pRM6qX96Popl87ftN2+tNkjeaNxah7iJlN5hkzu9CPX
MNemuwnjf5s3vDI+oNppcTSA3R6c451iOH9ZgYRso8NaCOsTHs2mbhcAEPkaP8xF
7OorZxmQq0ruSVDFn2MmuK0UzmFhoWHdM2MLGjkEDimYIGxMVb1MMMQmh1NF70nG
8QIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4E
FgQU46LJul+7sSUNX2Lu9Sl+mmyDAGgwEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZI
hvcNAQEFBQADggEBABbo22mWVeT3TQClauNBwKBaxw2EvOya5jnSpCkiKw4QYcPL
OfIe1zkwd0+/EFUysJwK6OeNawY8xxxHuEakTXXqjbEM8w5jXVUSo7rOLcTTM8rf
+EgelxQeSwgscLB+y774rMS9HissKjvu27+xbYRKh0GGZtwknKYiakQbisnQS4h8
HNCz9Nlnf3kv0ivpy7hxq4MTOBCyO8t7ThkMz8Z87YOGR1kptLM6JURZAKCusaTM
VulOcNSeaC8T7wkZFlgQpgbItHmI3vDHub0M8nzy8yNk/CNMLrAGnI9N6XYk7J9O
Zku3ouZNqiVgM2ngL2PzWp7RJ7raTOiN/EnW/R4=
-----END CERTIFICATE-----
quit
Certificate has the following attributes:
      Fingerprint MD5: 04F844EB B0A2D8BC A86E5543 05AC74EE
     Fingerprint SHA1: AF3C4ADD 14B13F10 CD50F7AD 8A3FE2EA CCE2227A

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

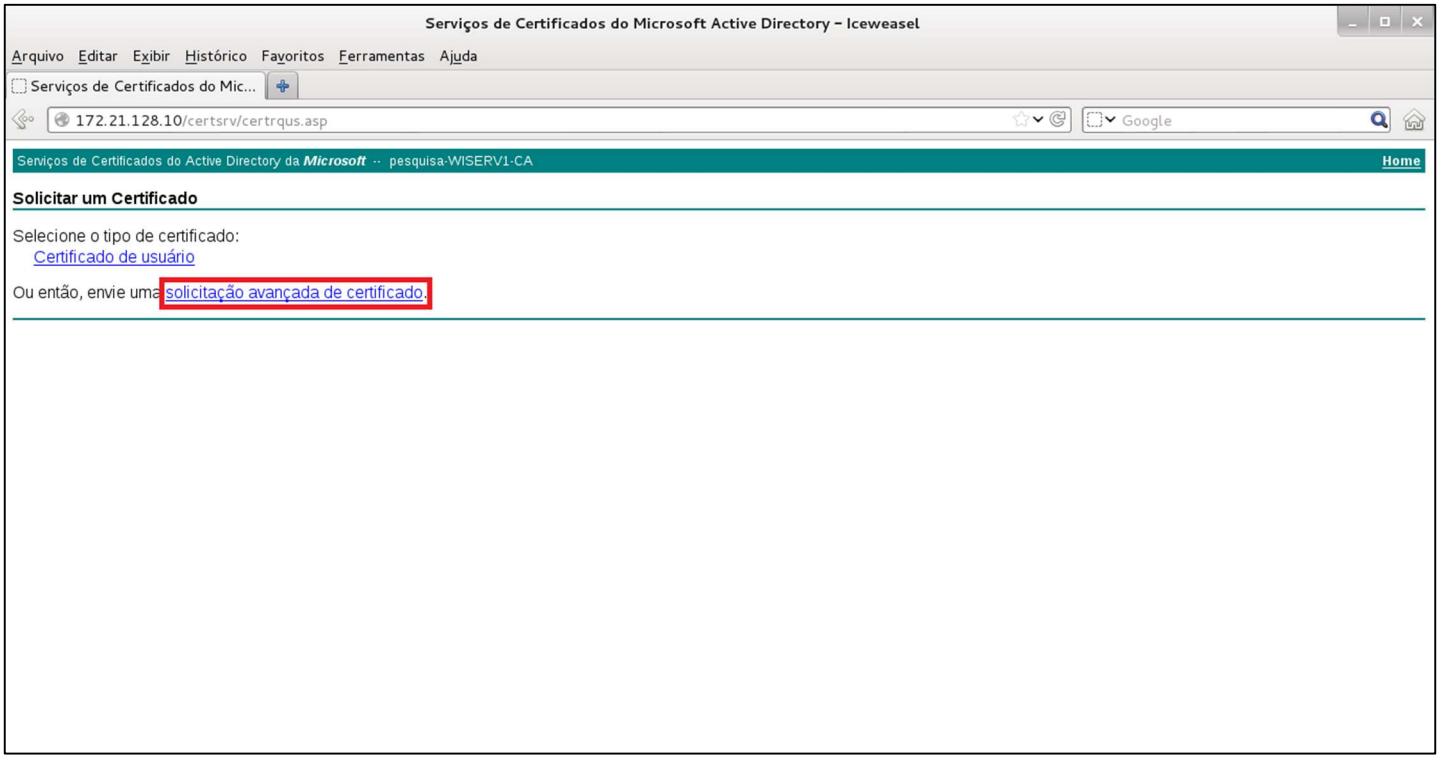
7. O comando abaixo gera uma requisição de certificado.

```
DCrot1(config)#crypto pki enroll CA
% Start certificate enrollment ..

% The subject name in the certificate will include: CN=DCrot1.pesquisa.local
% The subject name in the certificate will include: DCrot1.pesquisa.local
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

MIIBpzCCARACAQAwRjEeMBwGA1UEAxMVRENyb3QxLnBlc3F1aXNhLmxvY2FsMSQw
IgYJKoZIhvcNAQkCFhVEQ3JvdDEucGVzcXVpc2EubG9jYWwwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAPQs/f9mrLp7sNYzehWg44HbKR+NI8wyJRxc143UFr7n
JlCpCjoSPppXpVEnArUOPkwiR3+Nm9gQl4TA41DDgwglb5ta0iE5/kFROTRsJrKy
vKT23bbGPB5mr8wrvwp4Qsb0GE9vC+szUM0kiwj+tpehbkLCCvCcl2fljNnwm1UD
AgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQMA4GA1UdDwEB/wQEAwIFoDANBgkqhkiG
9w0BAQUFAAOBgQB8/qr0+LVJORAi5kSq8t+7R1JShXiI3Zkk3S26x0u+/6o6jYEp
sDP3lt2Xg0vw3AQ1h70S5q+FG1zjKhwsywdEOvHgm1A02v5l9ZmiT0wshHBZK2O8
dTeXgYdPOpR6l29QEEME7e1FYqcyT8zvo5TvL2DCHh33CZgV2gspUpT80A==

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
```

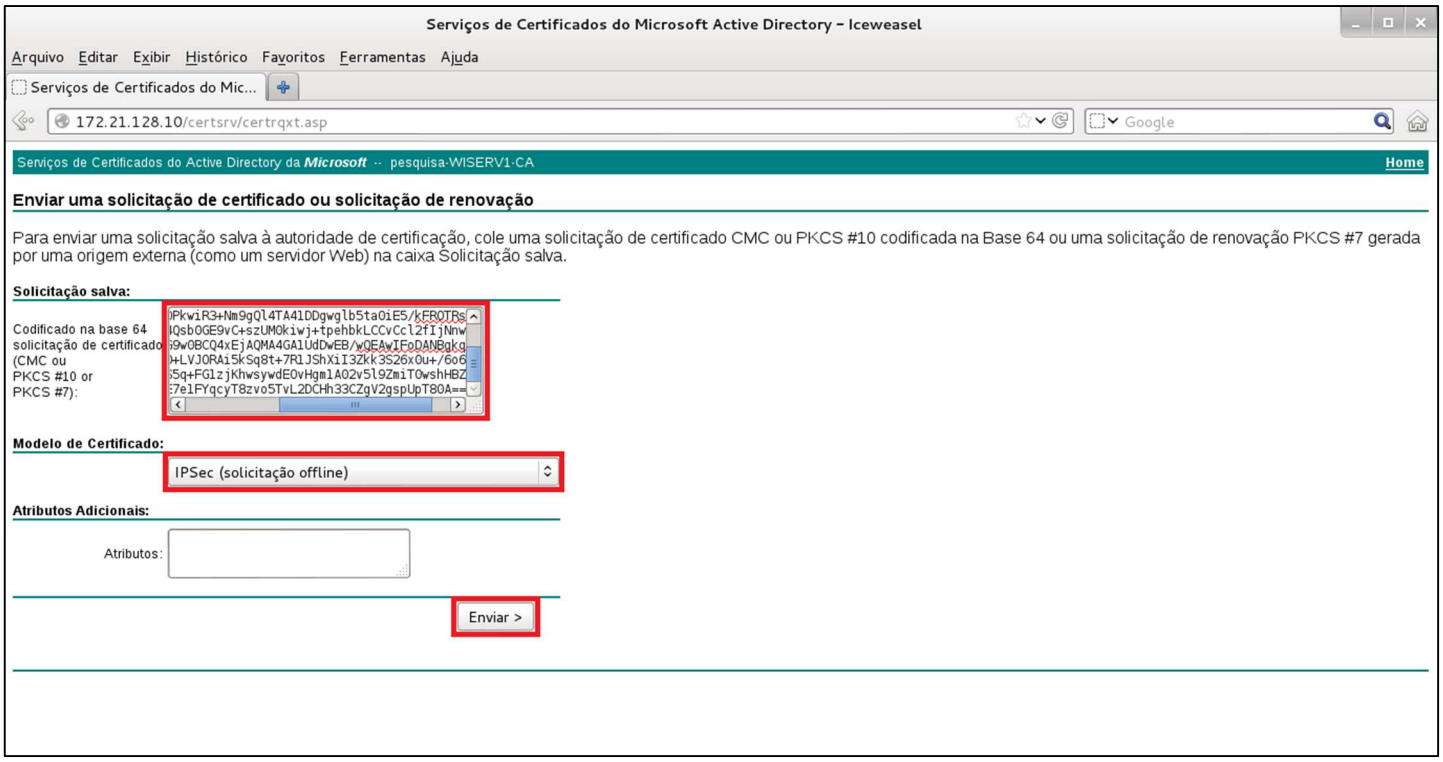
8. Na página principal da CA, clique em "**Solicitar um certificado**".



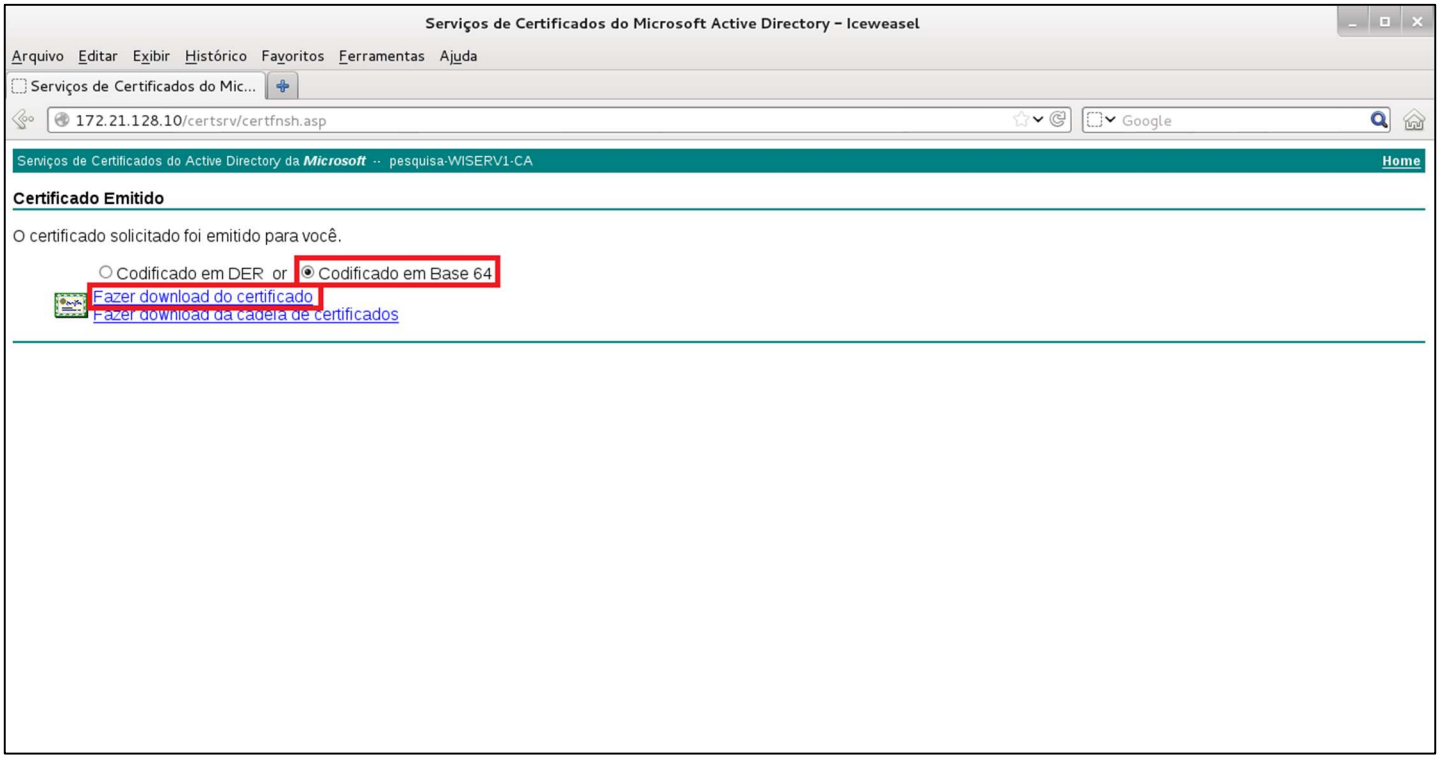
9. Clique em “**solicitação avançada de certificado**”.



10. Copie a requisição de certificado gerada no passo 7, cole no campo “**Certificado na base 64...**”, selecione o modelo “**IPSec (solicitação offline)**” e clique em “**Enviar**”.



11. Selecione “**Codificado em Base 64**” e clique em “**Fazer download do certificado**”.



12. Insira o comando abaixo para importar o certificado assinado pela CA. Copie o conteúdo do certificado obtido no passo 11 e cole no terminal. Após colar o conteúdo do certificado, pressione “**Enter**”, digite “**quit**” e pressione “**Enter**” novamente.

w DCrot1(config)#crypto pki import CA certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIE4zCCA8ugAwIBAgIKEVwpRQAAAAAASTANBgkqhkiG9w0BAQUFADBPMRUwEwYK
CZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghwZXNxdWlzYTEcMBoG
A1UEAxMTcGVzcXVpc2EtV0lTRVJWMS1DQTAeFw0xNDA2MDMxOTA0NThaFw0xNjA2
MDIxOTA0NThaMEYxJDAiBgkqhkiG9w0BCQITFURDcm90MS5wZXNxdWlzYS5sb2Nh
b24sREM9cGVzcXVpc2EsREM9bG9jYWw/Y0FDZXJ0aWZpY2F0ZT9iYXNlP29iamVj
dENsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkwPwYJKwYBBAGCNxQCBDIeMABJ
BgNVHSUEDDAKBggrBgEFBQgCAjANBgkqhkiG9w0BAQUFAAOCAQEAB2MuHBPo0irF
ofOE/N10ggvAswZvdRVEYNvz93EA/7AJszipmW9mihGHFd5BprqUxIo1wKxc9RnH
oXitwcQTrTSDhnew5Fb36UzME7fOu6Cj83yJrzFDltXH9DBxbILCo/8FvhAcVohg
xeB4M/rW/zzsXtqRuNXuYhgdvCJAdWY2zuXfCUCfVwDXAbi5RwBFj+73K01m3TUw
A6b9N3/YpMx0xxzhgZQV5LUKB30kQElAxU3FHjG6i0DTdtKsUQAtRyzs9jUwLYq3
s2Nx2hJ7ko2YNLi5HaZmjijZX4CnYcp8llPcgaas51Y0T6yg7Hb5moH5b7hVpkcD
ufEn0eufMw==
-----END CERTIFICATE-----
quit
% Router Certificate successfully imported

Configuração do IPSec

wqsec1

1. Para especificar o tráfego que será criptografado através do túnel IPSec é utilizado uma Lista de Acesso. O comando abaixo criar uma lista de acesso chamada "**VPN**" permitindo qualquer tráfego IP.

```
wqsec1(config)# access-list VPN extended permit ip any any
```

2. Para o estabelecimento de um túnel IPSec são utilizadas duas fases IKE: "**IKE Fase 1**" e "**IKE Fase 2**". Para configurar o "**IKE Fase 1**" e habilitá-lo utilize os comandos abaixo:

```
a. wqsec1(config)# crypto isakmp policy 10
b. wqsec1(config-isakmp-policy)# authentication rsa-sig
c. wqsec1(config-isakmp-policy)# encryption aes-256
d. wqsec1(config-isakmp-policy)# hash sha
e. wqsec1(config-isakmp-policy)# group 2
f. wqsec1(config-isakmp-policy)# lifetime 86400
   wqsec1(config-isakmp-policy)# exit

g. wqsec1(config)# crypto isakmp enable outside
```

a. Cria o mapa "**ISAKMP**" com prioridade "**10**"
b. Configura o método de autenticação usando Certificado Digital
c. Configura a criptografia "**AES256**"
d. Configura o algoritmo de integridade "**SHA**"
e. Configura o "**Diffie-Hellman 2**" para a troca de certificados
f. Configura o tempo de vida de "**86400**" segundos **(1 dia)** para o **SA (Security Association)**
g. Habilita o mapa ISAKMP na interface "**outside**"

3. Para configurar o "**IKE Fase 2**" e habilitá-lo utilize os comandos abaixo:

```
a. wqsec1(config)# crypto ipsec transform-set VPN esp-aes-256 esp-sha-hmac

b. wqsec1(config)# crypto map VPN 10 match address VPN
c. wqsec1(config)# crypto map VPN 10 set transform-set VPN
d. wqsec1(config)# crypto map VPN 10 set peer 91.16.63.114
e. wqsec1(config)# crypto map VPN 10 set trustpoint CA
f. wqsec1(config)# crypto map VPN interface outside
```

a. Configura o conjunto de parâmetros, "**transform-set**", com o nome "**VPN**" que será usado para o túnel "**IKE Fase 2**", isto é, túnel "**IPSec**".
b. Configura o Mapa de política "**VPN**" com prioridade "**10**" associando a Lista de Acesso "**VPN**" criada anteriormente. É nessa configuração que é identificado o tráfego que será criptografado.
c. Especifica o transform-set "**VPN**" para o mapa de política.
d. Especifica o endereço do par IPSec, ou seja, do outro equipamento.

e. Especifica o trustpoint que define o certificado para ser usado ao iniciar uma conexão com base nesta entrada
f. Habilita o mapa de política "**VPN**" na interface "**outside**"

4. No ASA é necessário criar um grupo de túnel para o túnel IPSec. Para configurar o grupo de túnel utilize os comandos abaixo:

a. wqsec1(config)# tunnel-group 91.16.63.114 type ipsec-l2l
b. wqsec1(config)# tunnel-group 91.16.63.114 ipsec-attributes
c. wqsec1(config-tunnel-ipsec)# trust-point CA
d. wqsec1(config-tunnel-ipsec)# peer-id-validate cert

a. Cria o grupo de túnel do tipo IPSec Site to Site, com o endereço do outro equipamento como identificação. **É necessário que a identificação seja o endereço IP do outro par IPsec.**
b. Acessa o modo de atributos IPSec do grupo de túnel.
c. Especifica o trust-point que identifica o certificado a ser enviado para o outro peer.
d. Configura para validar a identidade do peer usando o certificado do mesmo, se suportado pelo certificado.

DCrot1

1. Abaixo é criada uma lista de acesso chamada "**VPN**" para especificar o tráfego que será criptografado através do túnel IPSec. A lista de acesso especifica todo o tráfego IP.

DCrot1(config)#ip access-list extended VPN
DCrot1(config-ext-nacl)#permit ip any any
DCrot1(config-ext-nacl)#exit

2. Para a criação da "**IKE Fase 1**" são utilizados os comandos abaixo:

a. D DCrot1(config)#crypto isakmp policy 10
b. DCrot1(config-isakmp)#authentication rsa-sig
c. DCrot1(config-isakmp)#encryption aes 256
d. DCrot1(config-isakmp)#hash sha
e. DCrot1(config-isakmp)#group 2
f. DCrot1(config-isakmp)#lifetime 86400
DCrot1(config-isakmp)#exit

a. Cria o mapa "**ISAKMP**" com prioridade "**10**"
b. Configura o método de autenticação usando Certificado Digital
c. Configura a criptografia "**AES256**"
d. Configura o algoritmo de integridade "**SHA**"
e. Configura o "**Diffie-Hellman 2**" para a troca de chaves compartilhadas
f. Configura o tempo de vida de "**86400**" segundos **(1 dia)** para o **SA (Security Association)**

3. Para configurar o "**IKE Fase 2**", túnel IPSec, são utilizados os comandos abaixo:

a. D DCrot1(config)#crypto ipsec transform-set VPN esp-aes 256 esp-sha-hmac
   DCrot1(cfg-crypto-trans)#exit

b. DCrot1(config)#crypto map VPN 10 ipsec-isakmp
c. DCrot1(config-crypto-map)#match address VPN
d. DCrot1(config-crypto-map)#set peer 91.16.63.113
e. DCrot1(config-crypto-map)#set transform-set VPN
   DCrot1(config-crypto-map)#exit

a. Configura o conjunto de parâmetros, "**transform-set**", com o nome "**VPN**" que será usado para o túnel "**IKE Fase 2**", isto é, túnel "**IPSec**".
b. Configura o Mapa de política "**VPN**" com prioridade "**10**"
c. Especifica a lista de acesso "**VPN**" que indica o tráfego que será criptografado
d. Especifica o endereço do par IPSec, ou seja, do outro equipamento.
e. Especifica o transform-set "**VPN**" para o mapa de política.

4. Para habilitar o mapa de política na interface utilize os comandos abaixo:

```
DCrot1(config)#interface gigabitEthernet 0/0
DCrot1(config-if)#crypto map VPN
```

Nota: Antes de efetuar um teste de comunicação, verifique a data e horário de início e término da validade do certificado em cada equipamento, pois caso o horário e data do equipamento não esteja configurado entre o período de início e fim de validade, a comunicação não obterá sucesso. Para verificar o início e fim da validade do certificado utilize os comandos abaixo:

wqsec1

```
wqsec1# show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 11c81bea00000000004d
  Certificate Usage: General Purpose
  Public Key Type: RSA (1024 bits)
  Signature Algorithm: SHA1 with RSA Encryption
  Issuer Name:
    cn=pesquisa-WISERV1-CA
    dc=pesquisa
    dc=local
  Subject Name:
    cn=wqsec1.pesquisa.local
    hostname=wqsec1.pesquisa.local
  CRL Distribution Points:
    [1]  ldap:///CN=pesquisa-WISERV1-
CA,CN=wiserv1,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=pe
squisa,DC=local?certificateRevt
  Validity Date:
    start date: 21:02:53 UTC Jun 3 2014
    end   date: 21:02:53 UTC Jun 2 2016
  Associated Trustpoints: CA

CA Certificate
  Status: Available
  Certificate Serial Number: 626c8f3012b7839549136fe17cf122bd
  Certificate Usage: Signature
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA1 with RSA Encryption
  Issuer Name:
    cn=pesquisa-WISERV1-CA
    dc=pesquisa
    dc=local
  Subject Name:
    cn=pesquisa-WISERV1-CA
    dc=pesquisa
    dc=local
  Validity Date:
    start date: 11:40:33 UTC May 9 2014
    end   date: 11:50:30 UTC May 9 2019
  Associated Trustpoints: CA

wqsec1# clock set 21:16:00 03 JUN 2014
```

DCrot1

```
DCrot1#show crypto pki certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 11CD0DB900000000004E
  Certificate Usage: General Purpose
  Issuer:
    cn=pesquisa-WISERV1-CA
    dc=pesquisa
    dc=local
  Subject:
    Name: DCrot1.pesquisa.local
    cn=DCrot1.pesquisa.local
    hostname=DCrot1.pesquisa.local
  CRL Distribution Points:
    ldap:///CN=pesquisa-WISERV1-
CA,CN=wiserv1,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=pe
squisa,DC=local?certificateRevocatis
Jun  3 18:20:38.479: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
Jun  3 18:20:39.479: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to ups=cRLDistributionPoint
  Validity Date:
    start date: 21:08:17 UTC Jun 3 2014
    end   date: 21:08:17 UTC Jun 2 2016
  Associated Trustpoints: CA

CA Certificate
  Status: Available

DCrot1#clock set 21:20:55 03 JUN 2014
```

Verificação

Após efetuar um teste de comunicação entre os dois equipamentos, como por exemplo um "**ping**", siga os passos abaixo para verificar a funcionalidade do IPSec.

wqsec1

1. Verifica o "**IKE Fase 1**".

```
wqsec1# show crypto isakmp sa detail

  Active SA: 1
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 91.16.63.114
   Type    : L2L           Role    : responder
   Rekey   : no            State   : MM_ACTIVE
   Encrypt : aes-256       Hash    : SHA
   Auth    : rsa           Lifetime: 86400
   Lifetime Remaining: 86263
```

2. Verifica o "**IKE Fase 2**"

```
wqsec1# show crypto ipsec sa
interface: outside
   Crypto map tag: VPN, seq num: 1, local addr: 91.16.63.113

     access-list VPN extended permit ip any any
     local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     current_peer: 91.16.63.114

     #pkts encaps: 34, #pkts encrypt: 34, #pkts digest: 34
     #pkts decaps: 34, #pkts decrypt: 34, #pkts verify: 34
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 34, #pkts comp failed: 0, #pkts decomp failed: 0
     #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
     #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
     #send errors: 0, #recv errors: 0

     local crypto endpt.: 91.16.63.113, remote crypto endpt.: 91.16.63.114

     path mtu 1500, ipsec overhead 74, media mtu 1500
     current outbound spi: 63AA47C5
     current inbound spi : A59BD4AE
```

```
    inbound esp sas:
     spi: 0xA59BD4AE (2778453166)
       transform: esp-aes-256 esp-sha-hmac no compression
       in use settings ={L2L, Tunnel, }
       slot: 0, conn_id: 4096, crypto-map: VPN
       sa timing: remaining key lifetime (kB/sec): (3914996/3452)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000007 0xFFFFFFFF
    outbound esp sas:
     spi: 0x63AA47C5 (1672103877)
       transform: esp-aes-256 esp-sha-hmac no compression
       in use settings ={L2L, Tunnel, }
       slot: 0, conn_id: 4096, crypto-map: VPN
       sa timing: remaining key lifetime (kB/sec): (3914996/3452)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x00000001
```

DCrot1

1. Verifica o "**IKE Fase 1**"

```
DCrot1#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
     K - Keepalives, N - NAT-traversal
     T - cTCP encapsulation, X - IKE Extended Authentication
     psk - Preshared key, rsig - RSA signature
     renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local         Remote        I-VRF  Status Encr Hash   Auth DH Lifetime Cap.

1001  91.16.63.114    91.16.63.113         ACTIVE aes  sha    rsig 2  23:59:18
     Engine-id:Conn-id =  SW:1

IPv6 Crypto ISAKMP AS
```

2. Verifica o "**IKE Fase 2**"

```
DCrot1#show crypto ipsec sa

interface: GigabitEthernet0/0
   Crypto map tag: VPN, local addr 91.16.63.114

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 91.16.63.113 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29
   #pkts decaps: 29, #pkts decrypt: 29, #pkts verify: 29
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

    local crypto endpt.: 91.16.63.114, remote crypto endpt.: 91.16.63.113
    path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
    current outbound spi: 0xA59BD4AE(2778453166)
    PFS (Y/N): Y, DH group: none

    inbound esp sas:
     spi: 0x63AA47C5(1672103877)
       transform: esp-256-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2001, flow_id: Onboard VPN:1, sibling_flags 80000040, crypto map: VPN
       sa timing: remaining key lifetime (k/sec): (4229148/3530)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0xA59BD4AE(2778453166)
       transform: esp-256-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2002, flow_id: Onboard VPN:2, sibling_flags 80000040, crypto map: VPN
       sa timing: remaining key lifetime (k/sec): (4229148/3530)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)
```