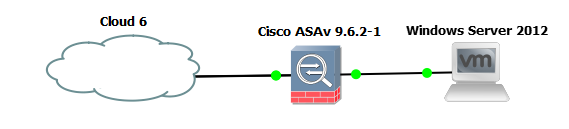
**AnyConnect**

Neste procedimento será demostrada a configuração do AnyConnect utilizando autenticação local, externa e por certificado. A topologia abaixo foi utilizada para o desenvolvimento deste procedimento:



Este procedimento resultará na seguinte configuração:

* Configurar AnyConnect VPN
  + Usar o range de endereços 20.0.0.0 – 20.0.0.100 /24 para os clientes
  + Permitir acesso somente endereço 10.0.0.2 (Windows Server)
  + Configurar Split-Tunneling
    - Apenas tráfego de roteamento para 10.0.0.2 atravessam o túnel VPN
  + Configurar para que o software VPN permaneça no cliente após a conexão ser fechada
  + Autenticar AnyConnect no Active Directory através do NPS e por certificado através da CA

Este procedimento está dividido em três partes:

* Configurar AnyConnect
* Testar AnyConnect
* Derrubar sessões AnyConnect

**Configurar AnyConnect**

1. Utilize os comandos abaixo para configurar o endereçamento da interface VLAN 1, utilizada para a Ethernet 0/0, e a interface VLAN 2, para Ethernet 0/1.

ASA(config)# interface vlan 1

ASA(config-if)# ip address 192.168.238.161 255.255.255.0

* 1. ASA(config-if)# nameif outside

ASA(config-if)# exit

ASA(config)# interface ethernet 0/0

ASA(config-if)# switchport access vlan 1

ASA(config-if)# no shutdown

ASA(config-if)# exit

ASA(config)# interface vlan 2

ASA(config-if)# ip address 10.0.0.1 255.255.255.0

* 1. ASA(config-if)# nameif inside

ASA(config-if)# exit

ASA(config)# interface ethernet 0/0

ASA(config-if)# switchport access vlan 2

ASA(config-if)# no shutdown

ASA(config-if)# exit

1. Define interface como “**outside**”, recebendo automaticamente o valor “**0**” para “**security-level**”.
2. Define interface como “**inside**”, recebendo automaticamente o valor “**100**” para “**security-level**”.
3. Configura o pool de endereços com nome “**ANYCONNECT**” que será distribuído aos clientes.

ASA(config)# ip local pool ANYCONNECT 20.0.0.1-20.0.0.100 mask 255.255.255.0

1. Configura o usuário para ser usado no Anyconnect

ASA(config)# username j.carlos password cisco

1. Cria um grupo de objeto com nome “**ANYCONNECT**”para identificar a rede dos endereços distribuídos aos clientes.

ASA(config)# object-group network ANYCONNECT

ASA(config-network)# network-object 20.0.0.0 255.255.255.0

ASA(config-network)# exit

1. Configura o WebVPN
2. ASA(config)# webvpn
3. ASA(config-webvpn)# enable outside
4. ASA(config-webvpn)# tunnel-group-list enable
5. ASA(config-webvpn)# anyconnect image disk0:/anyconnect-win-4.3.05017-k9.pkg 1
6. ASA(config-webvpn)# anyconnect enable

ASA(config-webvpn)# exit

1. Acessa o modo de configuração “**webvpn**”
2. Habilita o WebVPN na interface “**outside**”
3. Habilita a exibição de uma lista de grupos de túnel na página do WebVPN
4. Define uma imagem do AnyConnect com prioridade “**1**”. Sempre coloque com prioridade “**1**” a imagem compatível com a maioria dos sistemas operacionais que utilizarão o AnyConnect, pois esta será a primeira imagem disponibilizada para a instalação.
5. Habilita o uso das imagens AnyConnect
6. Habilita o redirecionamento HTTP para HTTPS

ASA(config)# http redirect outside

1. Cria uma ACL padrão permitindo pacotes com destino ao host 10.0.0.2. Neste caso, o cliente receberá somente uma rota /32 para o host em questão.

**Nota:** No Cisco ASA, a ACL padrão filtra os pacotes com base no endereço de destino e não no endereço de origem como os equipamentos que utilizam IOS (Router e Switch).

ASA(config)# access-list ROUTES standard permit host 10.0.0.2

1. Criar uma ACL com o tráfego que deverá ser permitido pela VPN. Caso você queira liberar todo o tráfego para as rotas que setou na ACL anterior, basta usar a mesma ACL.

ASA(config)# access-list ANYCONNECT extended permit tcp any host 10.0.0.2 eq 3389

ASA(config)# access-list ANYCONNECT extended permit tcp any host 10.0.0.2 eq 3389

ASA(config)# access-list ANYCONNECT extended permit tcp any host 10.0.0.2 eq 80

1. Cria uma política de grupo
2. ASA(config)# group-policy ANYCONNECT internal
3. ASA(config)# group-policy ANYCONNECT attributes
4. ASA(config-group-policy)# vpn-tunnel-protocol ssl-client
5. ASA(config-group-policy)# dns-server value 10.0.0.2
6. ASA(config-group-policy)# vpn-filter value ANYCONNECT
7. ASA(config-group-policy)# split-tunnel-policy tunnelspecified
8. ASA(config-group-policy)# split-tunnel-network-list value ROUTES
9. ASA(config-group-policy)# default-domain value cisco.local
10. Cria uma política de grupo interna com o nome “**ANYCONNECT**”.
11. Acessa o modo de atributos da política de grupo “**ANYCONNECT**”.
12. Permite o protocolo de túnel “**ssl-client**” para os clientes deste grupo.
13. Configura o endereço do servidor DNS utilizado para os clientes deste grupo.
14. Especifica a ACL que filtrará o tráfego na VPN, não há relação com as rotas que o cliente receberá.
15. Configura para que o túnel seja utilizado para comunicação apenas das redes especificadas no comando “**split-tunnel-network-list**”. Essa configuração cria rotas no cliente apenas para as redes especificadas. Necessário criar ACL standard.
16. Especifica a ACL que identifica o tráfego que utilizará o túnel.
17. Especifica o nome de domínio padrão para os clientes deste grupo.
18. Configura o grupo de túnel
19. ASA(config)# tunnel-group ANYCONNECT type remote-access
20. ASA(config)# tunnel-group ANYCONNECT general-attributes
21. ASA(config-tunnel-general)# default-group-policy ANYCONNECT
22. ASA(config-tunnel-general)# address-pool ANYCONNECT
23. ASA(config-tunnel-general)# authentication-server-group LOCAL

ASA(config-tunnel-general)# exit

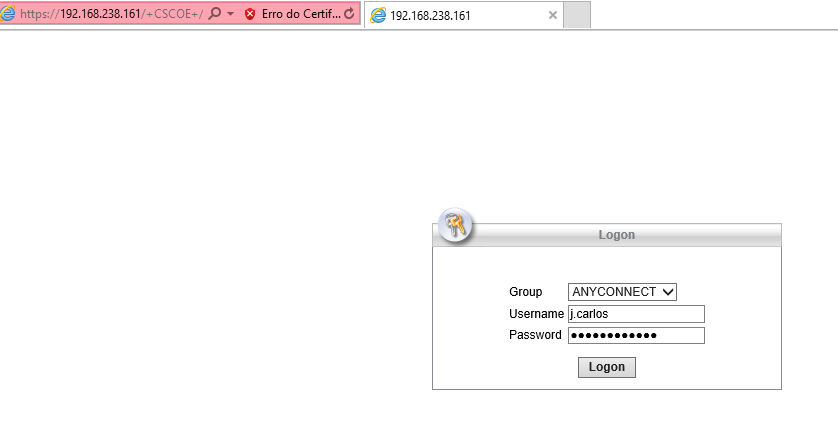
1. ASA(config)# tunnel-group ANYCONNECT webvpn-attributes
2. ASA(config-tunnel-webvpn)# group-alias ANYCONNECT

ASA(config-tunnel-webvpn)# exit

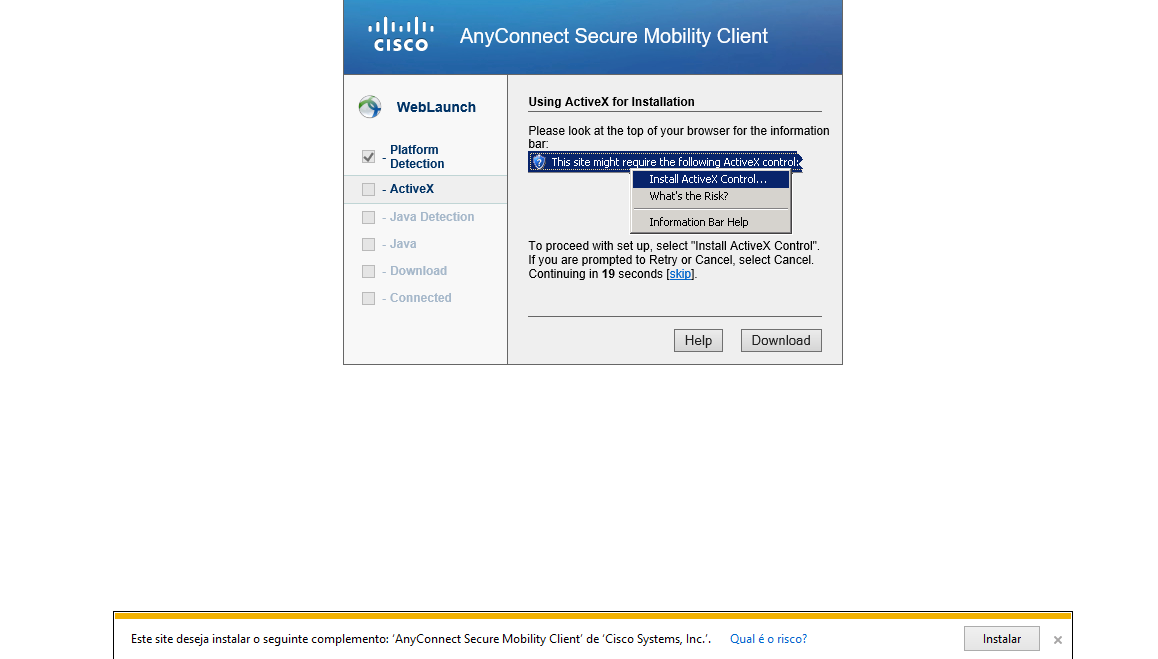
1. Cria um grupo de túnel com nome “**ANYCONNECT**” do tipo de acesso remoto.
2. Acessa o modo de atributos gerais do grupo de túnel “**ANYCONNECT**”.
3. Define a política de grupo padrão utilizada pelo grupo de túnel “**ANYCONNECT**”.
4. Define o pool de endereços distribuídos aos clientes que utilizarem o grupo de túnel “**ANYCONNECT**”.
5. Define a autenticação do Anyconnect com base local.
6. Acessa o modo de atributos WebVPN do grupo de túnel “**ANYCONNECT**”.
7. Define um alias para o grupo de túnel

**Testar AnyConnect**

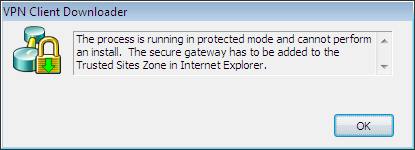
1. Utilizar o IE. No cliente, acesse o endereço [http://192.168.238.16](http://192.168.238.160)1 **(ip outside do asa).** Aceite o certificado auto-assinado e chegará na tela de login do Anyconnect



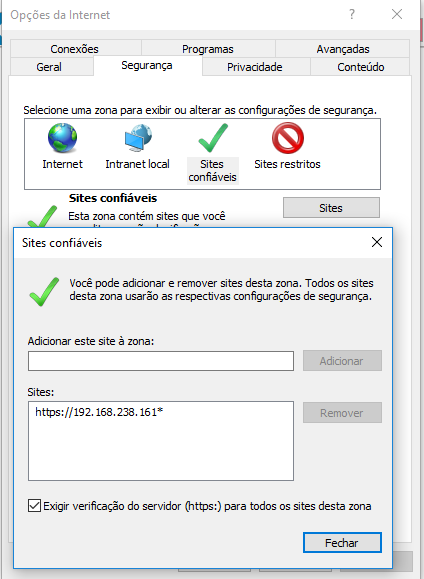
1. O instalador será iniciado automaticamente através do ActiveX. Será exibida a mensagem de certificado. Clique em “**Sim**” para continuar.



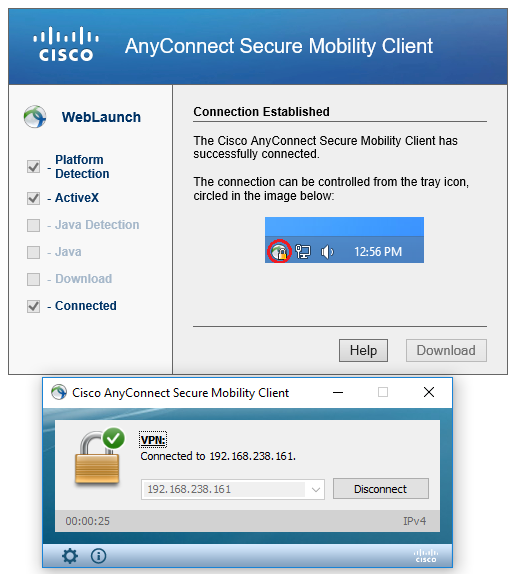
1. Será exibida a mensagem abaixo informando que o site não está configurado na zona de sites seguros do Internet Explorer. Clique em “**OK**”.



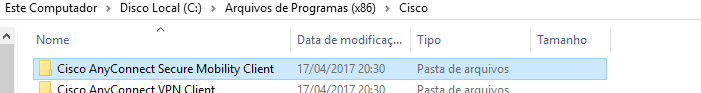
1. Adicione a URL “**https://192.168.238.161**” na zona de sites seguros do Internet Explorer.



1. Reinicie o navegador e efetue novamente os passos de 1 à 3. Desta vez a instalação será iniciada. Após efetuar a instalação, o instalador automaticamente efetuará a conexão VPN. Será informado que a VPN está conectada. Abra o software clicando duas vezes sobre o mesmo na área de notificações.



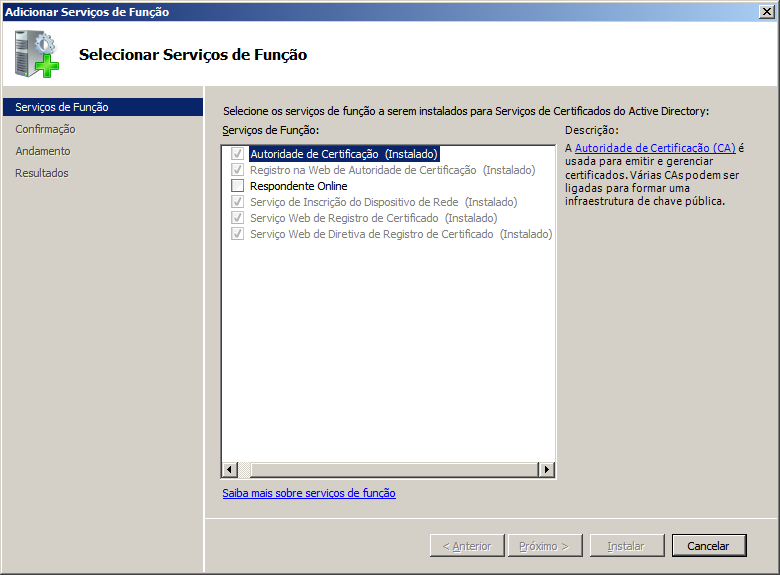
1. Note que o software foi instalado em “**C:\Arquivos de Programas\Cisco**”



**Utilizar autenticação por certificado e AAA**

Para utilizar autenticação por certificado e AAA, precisamos configurar uma CA para emitir e validar os certificados, um RADIUS (NPS) para integrar a autenticação com users do AD e configurar o ASA para utilize esses recursos. Na configuração abaixo será utilizado autoenrollment dos certificados, dessa forma, quando um usuário logar em uma máquina do AD, automaticamente receberá um User Certificate.

1. Para emitir e validar os certificados, é necessário que a função “**Serviços de Certificados do Active Directory**” e os serviços de função estejam instalados conforme imagem abaixo.



A autenticação do AnyConnect pode ocorrer somente através de certificado ou por Certificado e login, abaixo estarão as configurações à serem realizadas para autenticação dupla.

**Deploy automático de certificado de usuário ao logar no domínio.**

Use the Group Policy Management Console to configure user autoenrollment policy settings, and use the Certificate Templates snap-in to configure autoenrollment settings on the certificate template.

To automatically enroll client computers for certificates in a domain environment, you must:

* Configure an autoenrollment policy for the domain.
* Configure certificate templates for autoenrollment.
* Configure an enterprise CA.

Membership in **Domain Admins** or **Enterprise Admins** is required to complete these procedures.

### **To configure autoenrollment Group Policy for a domain**

1. On a domain controller, open the **Group Policy Management** console.
2. In the console tree, double-click **Group Policy Objects** in the forest and domain containing the **Default Domain Policy** Group Policy object (GPO) that you want to edit.
3. Right-click the**Default Domain Policy** GPO, and then click **Edit**.
4. In the Group Policy Management Console (GPMC), click **User Configuration**, **Policies**, **Windows Settings**, **Security Settings**, and then click **Public Key Policies**.
5. Double-click **Certificate Services Client - Auto-Enrollment**.
6. In **Configuration Model**, select **Enabled** to enable autoenrollment.
7. If you are enabling certificate autoenrollment, you can select the following check boxes:
   * **Renew expired certificates, update pending certificates, and remove revoked certificates**
   * **Update certificates that use certificate templates**
   * **Expiration notification**
8. Click **OK** to accept your changes.

### **To configure certificate templates for autoenrollment**

1. On the CA, open the Certification Authority snap-in.
2. Expand the CA. Right-click **Certificate Templates** and then click **Manage**.
3. Clone the certificate template that you want to enable for autoenrollment.
   1. We can clone the User Certificate Template.
4. On the **Action** menu, click **Properties**, and then click the **Security** tab.
5. Select or add the user or group that you want to permit for autoenrollment.
6. In the **Permissions for Authenticated Users** list, select **Read**, **Enroll**, and **Autoenroll** in the **Allow** column.
7. In the tab **Subject Name** and uncheck **Include e-mail name in subject name**, **E-mail name**

**To configure IPSEC certificate template for SCEP**

* 1. Clone IPSEC (Offline) template, in the tab **Extensions**, edit **Application Police** option and add **Server Authentication**.
  2. Add to the registry LOCAL\_MACHINE\SOFTWARE\microsoft\Cryptografy\MSCEP

The enterprise CA does not require autoenrollment configuration, but the certificate templates that you have enabled for autoenrollment must be assigned to the CA before client computers can automatically enroll for those certificates

.

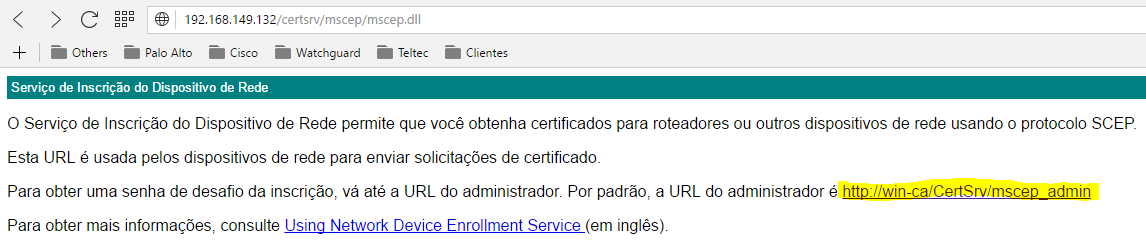
### **To assign certificate templates to an enterprise CA**

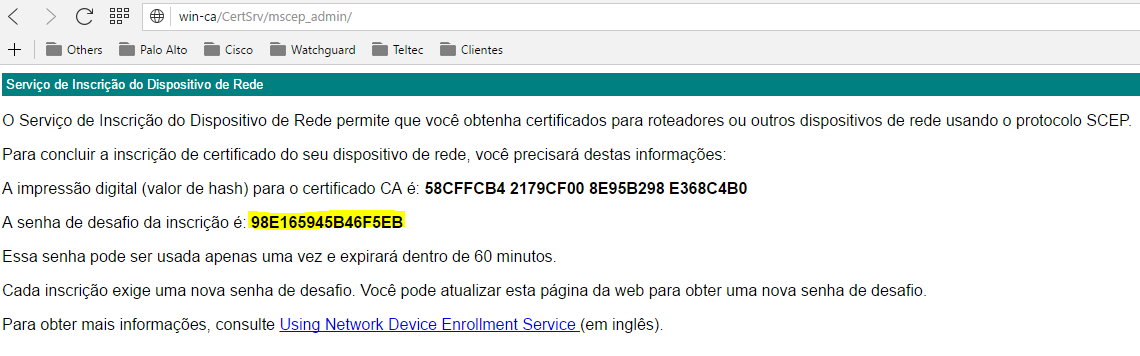
1. On the CA, open the Certification Authority snap-in.
2. In the console tree, click **Certificate Templates**.
3. On the **Action** menu, point to **New**, and then click **Certificate Template to Issue**.
4. Select the certificate template that you enabled for autoenrollment, and click **OK**.
5. Configura o AAA Server (NPS). Valide o funcionamento com o comando “test aaa” e debug aaa authentication.
6. ASA(config)# aaa-server radius protocol radius
7. ASA(config-aaa-server-group)# aaa-server radius (dmz) host 10.0.0.2
8. ASA(config-aaa-server-host)# key cisco
9. Modificar o tunnel-group general-attributes
   1. ASA(config)# tunnel-group anyconnect general-attributes
   2. ASA(config-tunnel-general)# username-from-certificate CN
   3. ASA(config-tunnel-general)# authentication-server-group radius
10. Acesse a política do tunnel-group general atributes
11. Com esta configuração, o anyconnect usará o parâmetro CN do certificado digital do cliente como usuário na conexão, dessa forma só necessário inserir a senha.
12. Configure para que o anyconnect utilize o radius configurado como servidor de autenticação.
13. É necessário agora configurar o ASA para que utilize a autenticação por certificado e por user/passwd.
14. ASA(config)# tunnel-group anyconnect webvpn-attributes
15. ASA(config-tunnel-webvpn)# authentication certificate aaa
16. ASA(config-tunnel-webvpn)# pre-fill-username client hide
17. Acesse a política do tunnel-group webvpn-attributes
18. **Configure a autenticação por certificado e por usuário/senha**
19. Ao configurar esse comando, é possível ocultar o usuário que está sendo autenticado no Anyconnect, lembrando que ele está sendo inserido automaticamente pelo ASA com o comando 1.b
20. Em caso de autenticação de certificado, é possível que o ASA sete automaticamente o login para um perfil de tunnel-group automaticamente, esse comando não é obrigatório.
21. ASA(config)# tunnel-group-map enable rules
22. ASA(config)# crypto ca certificate map anyconnect-map 10
23. ASA(config-ca-cert-map)# subject-name attr ou eq Cisco
24. Use the configured certificate map rules to match a certificate to a tunnel-group name
25. Crie um certificate map na entrada 10
26. Informe ao ASA que o atributo OU precisa ser igual a Cisco. É possível configurar outros parâmetros do certificado como CN, SCN, C, etc.
27. Em caso de autenticação de certificado, é possível que o ASA sete automaticamente o login para um perfil de tunnel-group, esse comando não é obrigatório.
28. ASA(config)# webvpn
29. ASA(config)# certificate-group-map anyconnect-map 10 anyconnect
30. Acesse a configuração de webvpn
31. Este comando informa ao ASA para mapear qualquer autenticação que de match com o map “ou=cisco” para o tunnel-group anyconnect
32. Configure o Windows Server como um CA trustpoint para que o ASA possa validar os certificados recebidos nas conexões.
    1. ASA(config)# crypto ca trustpoint CA
    2. ASA(config-ca-trustpoint)# enrollment url http://203.0.0.2:80/mscep/mscep.dll
    3. ASA(config-ca-trustpoint)# fqdn ASA.cisco.local
    4. ASA(config-ca-trustpoint)# subject-name CN=ASA.cisco.local
    5. ASA(config-ca-trustpoint)# keypair RSA-KEYS
    6. ASA(config-ca-trustpoint)# ignore-ipsec-keyusage
    7. ASA(config-ca-trustpoint)# password 99465E1EA3539FBC

ASA(config-ca-trustpoint)# exit

* 1. ASA(config)# ssl trust-point CA outside

1. Cria um trustpoint com o nome “**CA**”.
2. Configura o método de inscrição via url no formato http://ip\_ca:80/certsrv/mscep/mscep.dll
3. Configura o nome de domínio totalmente qualificado como “**ASA.cisco.local**”.
4. Configura o subject-name do trustpoint como “**CN=ASA.cisco.local**”.
5. Especifica o nome da chave gerada anteriormente para esta identidade.
6. Configura para suprimir o uso da chave verificando certificados de cliente IPSec. Comando necessário para evitar problemas com o check na CA, verificar o debug.
7. A senha à ser utilizada no comando password é utilizada para garantir a autenticidade do certificado assinado. Para obter essa key é necessário acessar a página do enrollment configurado no passo B e clicar no link “Obter uma senha de desafio da inscrição”:
8. Aplica o trustpoint na interface.





1. Insira o comando abaixo para importar o certificado da CA.

ASA(config)# crypto ca authenticate CA

INFO: Certificate has the following attributes:

Fingerprint: 58cffcb4 2179cf00 8e95b298 e368c4b0

Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

1. O comando abaixo gera uma requisição de certificado, assina e importa automaticamente.

ASA(config)# crypto ca enroll CA

% Start certificate enrollment ..

% The subject name in the certificate will be: CN=ASA.cisco.local

% The fully-qualified domain name in the certificate will be: ASA.cisco.local

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

Request certificate from CA? [yes/no]: yes

% Certificate request sent to Certificate Authority

ASA(config)# The certificate has been granted by CA!

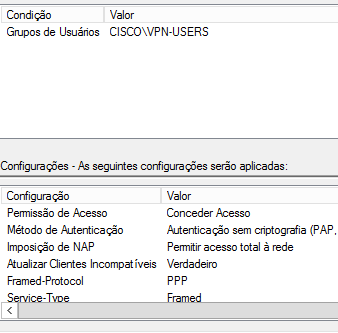
A partir desse ponto, a configuração de autenticação por AAA e certificate está pronta. O usuário receberá um certificado automaticamente do AD no login, ao conectar na VPN pelo Anyconnect, o ASA usará o CN desse certificado como username e só pedirá senha, após receber as credenciais, o ASA valida o usuário no NPS.

**Configuração do NPS**

1. Primeiramente, adicione o ASA como um cliente radius:



1. Adicione uma política de rede. Na aba Visão Geral, selecione **Conceder Acesso.** Na aba Condições, selecione o grupo de usuários que terá permissão para se autenticar na VPN. Na aba Restrições, no menu **Métodos de Autenticação,** selecione **Autenticação sem criptografia (CHAP)**



**Derrubar as conexões na web e anyconnect.**

1. Para derrubar as sessões webvpn insira o comando abaixo

ASA# vpn-sessiondb logoff webvpn

1. Para derrubar as sessões SVC insira o comando abaixo

ASA# vpn-sessiondb logoff anyconnect

**Show & Debug**

1. Mostra a configuração da VPN

ASA# show run tunnel-group anyconnect general-attributes / webvpn-attributes

ASA# show run group-policy anyconnect-group-policy

ASA# show run webvpn

ASA# show crypto ca certificate map anyconnect-map

1. Verificar status de conexão da VPN

ASA# show vpn-sessiondb anyconnect

ASA# show vpn-sessiondb detail anyconnect

ASA# show vpn-sessiondb webvpn

ASA# show vpn-sessiondb detail webvpn

1. Debug Webvpn & Anyconnect

ASA# debug webvpn 255

ASA# debug webvpn anyconnect 255

ASA# debug crypto vpnclient

1. Debug CA

ASA# debug crypto ca messages

ASA# debug crypto ca packets

ASA# debug crypto ca certificate

1. Para derrubar as sessões webvpn insira o comando abaixo

ASA# vpn-sessiondb logoff webvpn

1. Para derrubar as sessões Anyconnect insira o comando abaixo

ASA# vpn-sessiondb logoff anyconnect