Autenticação ASA 8.x Anyconnect com o cartão belga do eID

Índice

Introdução

Este documento descreve como estabelecer a autenticação ASA 8.x Anyconnect para usar o cartão belga do eID.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASA 5505 com o software apropriado ASA 8.0
- Cliente de AnyConnect
- ASDM 6.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

O eID é um cartão PKI (infraestrutura de chave pública) emitido pelo governo belga que os usuários devem usar a fim autenticar no as janelas remotas PC. O cliente de software de AnyConnect é instalado no PC local e toma credenciais de autenticação do PC remoto. Uma vez que a autenticação está completa, o usuário remoto acede aos recursos centrais através de um túnel completo SSL. O usuário remoto é fornecida com um endereço IP de Um ou Mais Servidores Cisco ICM NT obtido de um pool controlado pelo ASA.

Instalação do PC local

Sistema operacional

O sistema operacional (Windows, MacOS, Unix, ou Linux) em seu PC local deve ser atual com todas as correções requerida instaladas.

Leitor de cartão

Um leitor de cartão eletrônico deve ser instalado em seu computador local a fim usar o cartão do eID. O leitor de cartão eletrônico é um dispositivo de hardware que os establishs um canal de uma comunicação entre os programas no computador e a microplaqueta no ID cardem.

Para uma lista de leitores de cartão aprovados, refira esta URL:
http://www.cardreaders.be/en/default.htm

Nota: A fim usar o leitor de cartão, você deve instalar os direcionadores recomendados pelo fornecedor de hardware.

software do Runtime do eID

Você deve instalar o software do tempo de execução do eID fornecido pelo governo belga. Este software permite que o usuário remoto leia, valide, e imprima os índices do cartão do eID. O software está disponível em francês e em holandês para Windows, MAC OS X, e Linux.

Para mais informação, refira esta URL:

- http://www.belgium.be/zip/eid_datacapture_nl.html

Certificado da autenticação

Você deve importar o certificado da autenticação na loja de Microsoft Windows no PC local. Se você não importa o certificado na loja, o cliente de AnyConnect será incapaz de estabelecer uma conexão SSL ao ASA.

Procedimento

A fim importar o certificado da autenticação na loja de Windows, termine estas etapas:

1. Introduza seu eID no leitor de cartão, e lance o middleware a fim alcançar os índices do cartão do eID.Os índices do cartão do eID aparecem.
2. Clique a aba de **Certificats** (FR).A hierarquia dos Certificados é indicada.
3. Expanda a **CA raiz de Bélgica**, e expanda então o **cidadão CA.**
4. Escolha a versão da **autenticação de** seu certificado Nomeado.
5. Clique o botão de **Enregistrer** (FR).O certificado é copiado na loja de Windows.

Nota: Quando você clica o **botão Details Button**, um indicador parece que detalhes dos indicadores sobre o certificado. Nos detalhes catalogue, selecione o **campo de assunto** a fim ver o campo do número de série. O campo do número de série contém um valor exclusivo que seja usado para a autorização de usuário. Por exemplo, o número de série “56100307215" representa um usuário cuja a data de nascimento seja outubro ó, 1956 com um número de sequência de 072 e um dígito de verificação de 15. *Você deve submeter um pedido para a aprovação das autoridades federais a fim armazenar estes números. É sua responsabilidade fazer as declarações oficiais apropriadas relativas à manutenção de um base de dados de cidadãos belgas em seu país*.

Verificar

A fim verificar que o certificado importado com sucesso, termina estas etapas:

1. Em uma máquina de Windows XP, abra uma janela do dos, e datilografe o comando **mmc**.O aplicativo do console aparece.
2. Escolha o **> Add do arquivo/remova-o Pressão-em** (ou imprensa Ctrl+M).Adicionar/remove Pressão-na caixa de diálogo aparece.
3. Clique no botão Adicionar.Adicionar autônomo Pressão-na caixa de diálogo aparece.
4. Na lista Pressão-INS autônoma disponível, escolha **Certificados**, e o clique **adiciona**.
5. Clique **meu** botão de rádio da **conta de usuário**, e clique o **revestimento**.O certificado pressão-em aparece adicionar/remove Pressão-na caixa de diálogo.
6. O clique **próximo** a fim fechar adicionar autônomo Pressão-na caixa de diálogo, e clicar então a **APROVAÇÃO** adicionar/remove Pressão-na caixa de diálogo a fim salvar suas

mudanças e retornar ao aplicativo do console.
7. Sob a pasta da raiz de console, expanda **Certificados - Usuário atual**.
8. Expanda **pessoal**, e expanda então **Certificados**.O certificado importado deve aparecer na loja de Windows segundo as indicações desta imagem:

A instalação de AnyConnect

Você deve instalar o cliente de AnyConnect no PC remoto. O software de AnyConnect usa um arquivo de configuração XML que possa ser editado a fim pré-ajustar uma lista de gateways disponíveis. O arquivo XML é armazenado neste trajeto no PC remoto:

C:\Documents and Settings\ *%USERNAME%* \ dados do aplicativo \ Cisco \ Cisco AnyConnect VPN Client

onde *%USERNAME%* é o nome do usuário no PC remoto.

O nome do arquivo XML é *preferences.xml.* Está *aqui um* exemplo dos índices do arquivo:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectPreferences>
<DefaultHost>192.168.0.1</DefaultHost> </AnyConnectPreferences>
```

onde *192.168.0.1* é o endereço IP de Um ou Mais Servidores Cisco ICM NT do gateway ASA.

Exigências ASA

Assegure-se de que o ASA cumpra estas exigências:

- AnyConnect e o ASDM devem ser executado no flash.A fim terminar os procedimentos neste documento, use um ASA 5505 com o software apropriado ASA 8.0 instalado. O AnyConnect e os aplicativos ASDM devem ser preloaded no flash. Use o **comando show flash** a fim ver os índices do flash:`ciscoasa#show flash: --#-- --length-- -----date/time------ path 66 14524416 Jun 26 2007 10:24:02 asa802-k8.bin 67 6889764 Jun 26 2007 10:25:28 asdm-602.bin 68 2635734 Jul 09 2007 07:37:06 anyconnect-win-2.0.0343-k9.pkg`
- O ASA deve ser executado com padrões de fábrica.Você pode saltar esta exigência se você usa um chassi novo ASA a fim terminar os procedimentos neste documento. Se não, termine estas etapas a fim restaurar o ASA aos padrões de fábrica:No aplicativo ASDM, conecte ao chassi ASA, e escolha o **arquivo > dispositivo restaurado à configuração padrão de fábrica**.Deixe os valores padrão no molde.Conecte seu PC nos Ethernet 0/1 de interface interna, e renove seu endereço IP de Um ou Mais Servidores Cisco ICM NT que será fornecida pelo servidor DHCP do ASA.**Nota:** A fim restaurar o ASA aos padrões de fábrica da linha de comando, use estes comandos:`ciscoasa#conf t ciscoasa#config factory-default 192.168.0.1 255.255.255.0`

Configuração ASA

Uma vez que você restaura os padrões de fábrica ASA, você pode começar o ASDM a 192.168.0.1 a fim conectar ao ASA nos Ethernet 0/1 de interface interna.

Nota: Sua senha precedente é preservada (ou pode estar vazia à revelia).

Àrevelia, o ASA aceita uma nova sessão de gerenciamento com um endereço IP de origem na sub-rede 192.168.0.0/24. O servidor DHCP do padrão que é permitido na interface interna do ASA fornece endereços IP de Um ou Mais Servidores Cisco ICM NT na escala 192.168.0.2-129/24, válida para conectar à interface interna com o ASDM.

Termine estas etapas a fim configurar o ASA:

1. Permita a interface externa
2. Configurar o Domain Name, a senha, e o tempo de sistema
3. Permita um servidor DHCP na interface externa
4. Configurar o conjunto de endereços do eID VPN
5. Importe o certificado CA raiz de Bélgica
6. Configurar o secure sockets layer
7. Defina a política do grupo padrão
8. Defina o mapeamento do certificado
9. Adicionar um usuário local
10. Recarregue o ASA

Etapa 1. Permita a interface externa

Esta etapa descreve como permitir a interface externa.

1. No aplicativo ASDM, a **configuração do** clique, e clica então a **instalação de dispositivo**.
2. Na área de instalação do dispositivo, escolha **relações**, e clique então a aba das **relações**.
3. Selecione a interface externa, e o clique **edita**.
4. Na seção do endereço IP de Um ou Mais Servidores Cisco ICM NT do tab geral, escolha a opção do **IP Estático do uso**.
5. Entre em **197.0.100.1** para o endereço IP de Um ou Mais Servidores Cisco ICM NT e em **255.255.255.0** para a máscara de sub-rede.
6. Clique em Apply.

Etapa 2. Configurar o Domain Name, a senha, e o tempo de sistema

Esta etapa descreve como configurar o Domain Name, a senha, e o tempo de sistema.

1. Na área de instalação do dispositivo, escolha o **nome de dispositivo/senha**.
2. Incorpore **cisco.be para o** Domain Name, e incorpore cisco123for o valor de senha da possibilidade.**Nota:** À revelia, a senha está vazia.
3. Clique em Apply.
4. Na área de instalação do dispositivo, escolha o **tempo de sistema**, e mude o valor do pulso de disparo (caso necessário).
5. Clique em Apply.

Etapa 3. Permita um servidor DHCP na interface externa.

Esta etapa descreve como permitir um servidor DHCP na interface externa a fim facilitar testar.

1. **A configuração do** clique, e clica então o **Gerenciamento de dispositivos**.

2. Na área do Gerenciamento de dispositivos, expanda o **DHCP**, e escolha o **servidor DHCP**.
3. Selecione a interface externa da lista de interface, e o clique **edita**.A caixa de diálogo do servidor DHCP da edição aparece.
4. Verifique a caixa de verificação do **servidor DHCP da possibilidade**.
5. No pool de endereço DHCP, incorpore um endereço IP de Um ou Mais Servidores Cisco ICM NT de 197.0.100.20 a 197.0.100.30.
6. Na área global das opções de DHCP, desmarcar a **configuração automática da possibilidade da** caixa de **verificação de interface**.
7. Clique em Apply.

Etapa 4. Configurar o conjunto de endereços do eID VPN

Esta etapa descreve como definir um pool dos endereços IP de Um ou Mais Servidores Cisco ICM NT que são usados para provision os clientes remotos de AnyConnect.

1. **A configuração do** clique, e clica então o **acesso remoto VPN**.
2. Na área do VPN de acesso da remoção, expanda o **acesso da rede (cliente)**, e expanda então a **atribuição de endereço**.
3. Escolha **conjuntos de endereços**, e clique então o **botão Add** posicionado Configure nomeado área de associações do endereço IP de Um ou Mais Servidores Cisco ICM NT.A caixa de diálogo do IP pool adicionar aparece.
4. No campo de nome, incorpore o **EID-VPNPOOL**.
5. No endereço IP de Um ou Mais Servidores Cisco ICM NT começando e em terminar campos do endereço IP de Um ou Mais Servidores Cisco ICM NT, incorpore uma escala do endereço IP de Um ou Mais Servidores Cisco ICM NT de 192.168.10.100 a 192.168.10.110.
6. Escolha **255.255.255.0 da** lista de drop-down da máscara de sub-rede, clique a **APROVAÇÃO**, e clique-a então **aplicam-se**.

Etapa 5. Importe o certificado CA raiz de Bélgica

Esta etapa descreve como importar no ASA o certificado CA raiz de Bélgica.

1. Transfira e instale os certificados CA raiz de Bélgica (belgiumrca.crt e belgiumrca2.crt) do Web site do governo e armazene-os em seu PC local.O Web site do governo de Bélgica é ficado situado nesta URL: http://certs.eid.belgium.be/
2. Na área do acesso remoto VPN, expanda o **gerenciamento certificado**, e escolha **certificados de CA**.
3. O clique **adiciona**, e clica então **instala do arquivo**.
4. Consulte ao lugar em que você salvar o o arquivo do certificado CA raiz de Bélgica (belgiumrca.crt), e clique InstallCertificate**.**
5. O clique **aplica-se** a fim salvar suas mudanças.

Esta imagem mostra o certificado instalado no ASA:

Etapa 6. Configurar o secure sockets layer

Esta etapa descreve como dar a prioridade a opções de criptografia seguras, definir a imagem do cliente VPN SSL, e definir o perfil de conexão.

1. Dê a prioridade às opções de criptografia as mais seguras.Na área do acesso remoto VPN, expanda **avançado**, e escolha **ajustes SSL**. Na seção da criptografia, os algoritmos ativos são empilhados, parte superior para baixo, como segue:AES256-SHA1AES128-SHA13DES-SHA1RC4-SHA1
2. Defina a imagem do cliente VPN SSL para o cliente de AnyConnect.Na área do acesso remoto VPN, expanda **avançado**, expanda **SSL VPN**, e escolha **ajustes do cliente**.Na área das imagens do cliente VPN SSL, o clique **adiciona**.Escolha o pacote de AnyConnect que é armazenado no flash.O pacote de AnyConnect aparece no cliente VPN que SSL as imagens alistam segundo as indicações desta imagem:
3. Defina o perfil de conexão de DefaultWEBVPNGroup.Na área do acesso remoto VPN, expanda o **acesso da rede (cliente)**, e escolha **perfis da conexão de VPN SSL**.Na área das interfaces de acesso, verifique a **caixa de verificação do Cisco AnyConnect VPN Client da possibilidade**.Para a interface externa, verifique o **acesso reservar**, **exija o certificado de cliente**, e **permita** caixas de seleção **DTL** segundo as indicações desta imagem:Na área dos perfis de conexão, escolha **DefaultWEBVPNGroup**, e o clique **edita**.A caixa de diálogo do perfil da conexão de VPN da edição SSL aparece.Na área da navegação, escolha **básico**.Na área da autenticação, clique o botão de rádio do **certificado**.Na área de política do grupo padrão, verifique a caixa de verificação do **protocolo do cliente VPN SSL**.Expanda **avançado**, e escolha a **autenticação**.O clique **adiciona**, e adiciona a interface externa com um grupo de servidor local segundo as indicações desta imagem:Na área da navegação, escolha a **autorização**.Na área do grupo de servidor de autorização do padrão, escolha o **LOCAL da** lista de drop-down do grupo de servidor, e verifique os **usuários deve existir no base de dados da autorização para conectar a** caixa de verificação.No nome de usuário que traça a área, escolha **SER (número de série) da** lista de drop-down do campo do DN principal, não escolha **nenhuns do** campo do DN secundário, e clique a **APROVAÇÃO**.

Etapa 7. Defina a política do grupo padrão

Esta etapa descreve como definir a política do grupo padrão.

1. Na área do acesso remoto VPN, expanda o **acesso da rede (cliente)**, e escolha **políticas do grupo**.
2. Escolha o **DfltGrpPolicy da** lista de políticas do grupo, e o clique **edita**.
3. A caixa de diálogo da Política interna de grupo da edição aparece.
4. Da área da navegação, escolha o **general**.
5. Para conjuntos de endereços, clique **seleto** a fim escolher um conjunto de endereço, e escolha o **EID-VPNPOOL**.
6. Em mais área das opções, desmarcar as caixas de seleção do **IPsec** e **L2TP/IPsec**, e clique a **APROVAÇÃO**.

Etapa 8. Defina o mapeamento do certificado

Esta etapa descreve como definir os critérios do mapeamento do certificado.

1. Na área do acesso remoto VPN, clique **avançado**, e escolha o **certificado aos mapas do perfil da conexão de VPN SSL**.
2. No certificado à área dos mapas do perfil de conexão, o clique **adiciona**, e escolhe **DefaultCertificateMap da** lista do mapa.Este mapa deve combinar *DefaultWEBVPNProfile no*

traçado ao campo do perfil de conexão.
3. Na área de critérios de traço, o clique **adiciona**, e adiciona estes valores:Campo: O expedidor, o país (c), iguais, “seja”Campo: Expedidor, Common Name (CN), iguais, “cidadão Ca”Os critérios do mapeamento devem aparecer segundo as indicações desta imagem:
4. Clique em Apply.

Etapa 9. Adicionar um usuário local

Esta etapa descreve como adicionar um usuário local.

1. Na área do acesso remoto VPN, expanda a **instalação AAA**, e escolha **usuários locais**.
2. Na área de usuários locais, o clique **adiciona**.
3. No campo de nome de usuário, incorpore o número de série do certificado de usuário. Por exemplo, 56100307215 (como descrito na seção do certificado da autenticação deste documento).
4. Clique em Apply.

Etapa 10. Recarregue o ASA

Recarregue o ASA a fim assegurar-se de que todas as mudanças estejam aplicadas aos serviços de sistema.

Ajustar

Ao testar, alguns túneis SSL não puderam fechar-se corretamente. Desde que o ASA supõe que o cliente de AnyConnect pode desligar e reconectar, o túnel não é deixado cair, que lhe dá uma possibilidade voltar. Contudo, durante testes de laboratório com uma licença baixa (2 túneis SSL à revelia), você pôde esgotar sua licença quando os túneis SSL não são fechados corretamente. Se esta edição ocorre, use o **<option > o** comando do **fazer logoff VPN-sessiondb** a fim terminar todas as sessões de SSL ativas.

Configuração do minuto

A fim criar rapidamente uma configuração em funcionamento, restaure seu ASA ao padrão de fábrica, e cole esta configuração no modo de configuração:

ciscoasa

```
ciscoasa#conf t ciscoasa#clear configure all
ciscoasa#domain-name cisco.be ciscoasa#enable password
9jNfZuG3TC5tCVH0 encrypted ! interface Vlan1 nameif
inside security-level 100 ip address 192.168.0.1
255.255.255.0 interface Vlan2 nameif outside security-
level 0 ip address 197.0.100.1 255.255.255.0 interface
Ethernet0/0 switchport access vlan 2 no shutdown
interface Ethernet0/1 no shutdown ! passwd
2KFQnbNIdI.2KYOU encrypted dns server-group DefaultDNS
domain-name cisco.be ip local pool eID-VPNPOOL
192.168.10.100-192.168.10.110 mask 255.255.255.0 asdm
image disk0:/asdm-602.bin no asdm history enable global
(outside) 1 interface nat (inside) 1 0.0.0.0 0.0.0.0
dynamic-access-policy-record DfltAccessPolicy http
```

```
server enable http 192.168.0.0 255.255.255.0 inside
crypto ca trustpoint ASDM_TrustPoint0 enrollment
terminal crl configure crypto ca certificate map
DefaultCertificateMap 10 issuer-name attr c eq be
issuer-name attr cn eq citizen ca crypto ca certificate
chain ASDM_TrustPoint0 certificate ca
580b056c5324dbb25057185ff9e5a650 30820394 3082027c
a0030201 02021058 0b056c53 24dbb250 57185ff9 e5a65030
0d06092a 864886f7 0d010105 05003027 310b3009 06035504
06130242 45311830 16060355 0403130f 42656c67 69756d20
526f6f74 20434130 1e170d30 33303132 36323330 3030305a
170d3134 30313236 32333030 30305a30 27310b30 09060355
04061302 42453118 30160603 55040313 0f42656c 6769756d
20526f6f 74204341 30820122 300d0609 2a864886 f70d0101
01050003 82010f00 3082010a 02820101 00c8a171 e91c4642
7978716f 9daea9a8 ab28b74d c720eb30 915a75f5 e2d2cfc8
4c149842 58adc711 c540406a 5af97412 2787e99c e5714e22
2cd11218 aa305ea2 21b9d9bb fff674eb 3101e73b 7e580f91
164d7689 a8014fad 226670fa 4b1d95c1 3058eabc d965d89a
b488eb49 4652dfd2 531576cb 145d1949 b16f6ad3 d3fdbcc2
2dec453f 093f58be fcd4ef00 8c813572 bff718ea 96627d2b
287f156c 63d2caca 7d05acc8 6d076d32 be68b805 40ae5498
563e66f1 30e8efc4 ab935e07 de328f12 74aa5b34 2354c0ea
6ccefe36 92a80917 eaa12dcf 6ce3841d de872e33 0b3c74e2
21503895 2e5ce0e5 c631f9db 40fa6aa1 a48a939b a7210687
1d27d3c4 a1c94cb0 6f020301 0001a381 bb3081b8 300e0603
551d0f01 01ff0404 03020106 300f0603 551d1301 01ff0405
30030101 ff304206 03551d20 043b3039 30370605 60380101
01302e30 2c06082b 06010505 07020116 20687474 703a2f2f
7265706f 7369746f 72792e65 69642e62 656c6769 756d2e62
65301d06 03551d0e 04160414 10f00c56 9b61ea57 3ab63597
6d9fddb9 148edbe6 30110609 60864801 86f84201 01040403
02000730 1f060355 1d230418 30168014 10f00c56 9b61ea57
3ab63597 6d9fddb9 148edbe6 300d0609 2a864886 f70d0101
05050003 82010100 c86d2251 8a61f80f 966ed520 b281f8c6
dca31600 dacd6ae7 6b2afa59 48a74c49 37d773a1 6a01655e
32bde797 d3d02e3c 73d38c7b 83efd642 c13fa8a9 5d0f37ba
76d240bd cc2d3fd3 4441499c fd5b29f4 0223225b 711bbf58
d9284e2d 45f4dae7 b5634544 110d2a7f 337f3649 b4ce6ea9
0231ae5c fdc889bf 427bd7f1 60f2d787 f6572e7a 7e6a1380
1ddce3d0 631e3d71 31b160d4 9e08caab f094c748 755481f3
1bad779c e8b28fdb 83ac8f34 6be8bfc3 d9f543c3 6455eb1a
bd368636 ba218c97 1a21d4ea 2d3bacba eca71dab beb94a9b
352f1c5c 1d51a71f 54ed1297 fff26e87 7d46c974 d6efeb3d
7de6596e 069404e4 a2558738 286a225e e2be7412 b004432a
quit no crypto isakmp nat-traversal ! dhcpd address
192.168.0.2-192.168.0.129 inside dhcpd enable inside
dhcpd address 197.0.100.20-197.0.100.30 outside dhcpd
enable outside ! service-policy global_policy global ssl
encryption aes256-sha1 aes128-sha1 3des-sha1 rc4-sha1
ssl certificate-authentication interface outside port
443 webvpn enable outside svc image disk0:/anyconnect-
win-2.0.0343-k9.pkg 1 svc enable certificate-group-map
DefaultCertificateMap 10 DefaultWEBVPNGroup group-policy
DfltGrpPolicy attributes vpn-tunnel-protocol svc webvpn
address-pools value eID-VPNPOOL username 63041403325
nopassword tunnel-group DefaultWEBVPNGroup general-
attributes authentication-server-group (outside) LOCAL
authorization-server-group LOCAL authorization-required
authorization-dn-attributes SER tunnel-group
DefaultWEBVPNGroup webvpn-attributes authentication
certificate exit copy run start
```

Informações Relacionadas

- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems