ASA 8.x: Configuração das CAC-carta inteligente de AnyConnect SSL VPN com apoio MAC

Índice

Introdução

Este documento fornece uma configuração de exemplo na ferramenta de segurança adaptável de Cisco (ASA) para o Acesso remoto de AnyConnect VPN para o apoio MAC com o cartão comum do acesso (CAC) para a autenticação.

O espaço deste documento é cobrir a configuração de Cisco ASA com o Directory Access Protocol adaptável do Security Device Manager (ASDM), do Cisco AnyConnect VPN Client e do microsoft ative directory (AD) /Lightweight (LDAP).

A configuração neste guia usa o server de Microsoft AD/LDAP. Este documento igualmente cobre recursos avançados tais como OCSP, mapas do atributo LDAP e o acesso dinâmico policia (DAP).

Pré-requisitos

Requisitos

Uma compreensão básica do cliente de Cisco ASA, de Cisco AnyConnect, do Microsoft AD/LDAP e do Public Key Infrastructure (PKI) é benéfica na compreensão da instalação completa. A familiaridade com a membrasia do clube AD, as propriedades de usuário assim como os objetos LDAP ajudam na correlação do processo da autorização entre atributos do certificado e objetos AD/LDAP.

Componentes Utilizados

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

- A ferramenta de segurança adaptável do Cisco 5500 Series (ASA) essa executa a versão de software 8.0(x) e mais atrasada

- Versão 6.x do Cisco Adaptive Security Device Manager (ASDM) para ASA 8.x
- Cisco AnyConnect VPN Client 2.2 com apoio MAC

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.

Configuração ASA Cisco

Esta seção cobre a configuração de Cisco ASA através do ASDM. Cobre as etapas necessárias a fim distribuir um túnel de acesso remoto VPN através de uma conexão SSL AnyConnect. O certificado CAC é usado para a autenticação e o atributo do nome principal do usuário (UPN) no certificado é povoado no diretório ativo para a autorização.

Considerações de desenvolvimento

- Este guia não cobre configurações básicas tais como relações, DNS, NTP, roteamento, acesso de dispositivo, acesso ASDM e assim por diante. Supõe-se que o operador de rede é familiar com estas configurações.Refira ferramentas de segurança Multifunction para mais informação.
- As seções destacadas no VERMELHO são configurações imperativas necessárias para o acesso básico VPN. Por exemplo, um túnel VPN pode ser setup com o cartão CAC sem fazer verificações OCSP, mapeamentos LDAP e verificações da política do acesso dinâmico (DAP). Os mandatos verificação OCSP do DoD mas o túnel trabalham sem OCSP configurado.
- As seções destacadas no AZUL são os recursos avançados que podem ser incluídos para adicionar mais Segurança ao projeto.
- O ASDM e AnyConnect/SSL VPN não podem usar as mesmas portas na mesma relação. Recomenda-se mudar as portas em uma ou as outro para aceder. Por exemplo, use a porta 445 para o ASDM e deixe 443 para AC/SSL VPN. O acesso ASDM URL mudou em 8.x. Use o `<ip_address> de https://: <port>/admin.html`.
- A imagem ASA exigida é pelo menos 8.0.2.19 e ASDM 6.0.2.
- AnyConnect/CAC é apoiado com vista.
- Veja o apêndice A para o LDAP & os exemplos do mapeamento da política do acesso dinâmico para o reforço de política adicional.
- Veja o apêndice D em como verificar objetos LDAP no MS.
- Veja a informação relacionada para portas de uma lista de aplicativo para a configuração de firewall.

Autenticação, autorização, configuração (AAA) explicando

Você é autenticado com o uso do certificado em seu cartão comum do acesso (CAC) através do

server da autoridade de DISACertificate (CA) ou do server de CA de sua própria organização. O certificado deve ser válido para o Acesso remoto à rede. Além do que a autenticação, você deve igualmente ser autorizado usar um objeto do microsoft ative directory ou do Lightweight Directory Access Protocol (LDAP). O departamento de defesa (DoD) exige o uso do atributo do nome principal de usuário (UPN) para a autorização, que é parte da seção alternativa sujeita do nome (SAN) do certificado. O UPN ou o EDI/PI devem estar neste formato, 1234567890@mil. Estas configurações mostram como configurar o servidor AAA no ASA com um servidor ldap para a autorização. Veja o apêndice A para a configuração adicional com LDAP objetar o mapeamento.

Configurar o servidor ldap

Conclua estes passos:

1. Escolha o **acesso remoto VPN > o AAA Setup > Grupo de servidores AAA.**
2. Nos Grupos de servidores AAA apresente, clique **adicionam 3.**
3. Dê entrada com o nome do grupo de servidor e escolha o **LDAP no** botão Protocol Radio Button. Veja figura 1.
4. Nos server na tabela selecionada do grupo, o clique **adiciona**. Certifique-se de que o server que você criou está destacado na tabela precedente.
5. No indicador do servidor AAA da edição, termine estas etapas. Veja figura 2.**Nota:** Escolha a **possibilidade LDAP sobre a opção de SSL** se seu LDAP/AD é configurado para este tipo de conexão.Escolha a relação onde o LDAP é encontrado. Este guia mostra dentro da relação.Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do server.Entre na **porta de servidor**. A porta do padrão LDAP é 389.Escolha o **tipo de servidor**.Incorpore o **DN baixo**. Peça seu administrador AD/LDAP estes valores.**Figure-1**Sob a opção de escopo, escolha a resposta apropriada. Isto é dependente da base DN. Peça seu administrador AD/LDAP o auxílio.No atributo de nomeação, incorpore o **userPrincipalName**. Este é o atributo que é usado para a autorização de usuário no server AD/LDAP.No início de uma sessão DN, incorpore o DN do Administrador.**Nota:** Você tem direitos administrativos ou opinião dos direitos/busca a estrutura LDAP que inclui objetos do usuário e membrasia do clube.Na senha de login, incorpore a senha do administrador.Deixe o atributo LDAP a **nenhuns**.**Figure-2 Nota:** Você usa esta opção mais tarde a configuração para adicionar o outro objeto AD/LDAP para a autorização.Escolha **ESTÁ BEM**.
6. Escolha **ESTÁ BEM**.

Controle Certificados

Há duas etapas a fim instalar Certificados no ASA. Primeiramente, instale os certificados de CA (Certificate Authority da raiz e do subordinado) precisou. Em segundo lugar, registre o ASA a um específico CA e obtenha o certificado de identidade. O DoD PKI utiliza estes Certificados, raiz CA2, raiz da classe 3, intermediário CA## que o ASA está registrado com, certificado ASA ID e certificado OCSP. Mas, se você escolhe não usar OCSP, o certificado OCSP não precisa de ser instalado.

Nota: Contacte seu POC da Segurança a fim obter certificados de raiz assim como instruções em como registrar-se para um certificado de identidade para um dispositivo. Um certificado SSL deve ser suficiente para o ASA para o Acesso remoto. Um certificado duplo SAN não é exigido.

Nota: A máquina local igualmente tem que ter a corrente de CA do DoD instalada. Os Certificados

podem ser vistos na loja do certificado de Microsoft com o internet explorer. O DoD produziu um arquivo de lote que adicionasse automaticamente todos os CA à máquina. Peça seu POC PKI mais informação.

Nota: O DoD CA2 e a classe 3 enraízam assim como o intermediário ASA ID e de CA que emitiu o CERT ASA deve ser os únicos CA necessários para a autenticação de usuário. Todos os intermediários atuais de CA caem sob a corrente da raiz CA2 e de classe 3 e são confiados enquanto as raizes CA2 e de classe 3 são adicionadas.

Gerencia chaves

Conclua estes passos:

1. Escolha o **> gerenciamento de certificado do acesso remoto VPN > o > Add do certificado de identidade**.
2. Escolha **adicionam um certificado novo identificação** e então **novo pela** opção do par de chaves.
3. No indicador do par de chaves adicionar, dê entrada com um nome chave, **DoD-1024**. Clique sobre o rádio para adicionar uma chave nova. Consulte a figura 3.**Figura 3**
4. Escolha o tamanho da chave.
5. Mantenha o uso ao **uso geral**.
6. O clique **gerencie agora**.**Nota:** A CA raiz 2 do DoD usa uma chave de 2048 bit. Uma segunda chave que use um par de chaves de 2048 bit deve ser gerada para poder usar este CA termina o precedente acima das etapas a fim adicionar uma segunda chave.

Instale certificados CA raiz

Conclua estes passos:

1. Escolha o **> gerenciamento de certificado do acesso remoto VPN > o > Add do certificado de CA**.
2. Escolha **instalam do arquivo** e consultam ao certificado.
3. Escolha **instalam o certificado**.**Figura 4: Instalando o certificado de raiz**
4. Este indicador deve aparecer. Veja a figura 5.**Figura 5 Nota:** Repita etapas 1 a 3 para cada certificado que você quer instalar. O DoD PKI exige um certificado para cada um destes: CA raiz 2, raiz da classe 3, intermediário CA##, server ASA ID e OCSP. O certificado OCSP não é precisado se você não usa OCSP.**Figura 6: Instalando o certificado de raiz**

Registre o ASA e instale o certificado de identidade

1. Escolha o **> gerenciamento de certificado do acesso remoto VPN > o > Add do certificado de identidade**.
2. Escolha **adicionam um certificado novo identificação**.
3. Escolha o par de chaves do **DoD-1024**. Veja a figura 7**Figura 7: Parâmetros do certificado de identidade**
4. Vá à caixa do assunto DN do certificado e clique **seleto**.
5. No indicador do assunto DN do certificado, incorpore a informação do dispositivo. Veja figura 8 por exemplo.**Figura 8: Edite o DN**

6. Escolha **ESTÁ BEM**.**Nota:** Certifique-se de que você usa o hostname do dispositivo que está configurado em seu sistema quando você adicionar o assunto DN. O POC PKI pode dizer-lhe os campos imperativos exigidos.
7. Escolha **adicionam o certificado**.
8. O clique **consulta** a fim selecionar o diretório onde você quer salvar o pedido. Veja a figura 9.**Figure o pedido do certificado 9**
9. Abra o arquivo com WordPad, copie o pedido à documentação apropriada e envie-o a seu POC PKI. Veja a figura 10.**Figura 10: Pedido do registro**
10. Uma vez que você recebeu o certificado do administrador de CA, escolha o **> gerenciamento de certificado do acesso remoto VPN > o certificado ID > instalam**. Veja figura 11.**Figura 11: Importando o certificado de identidade**
11. No indicador do certificado da instalação, consulte ao **certificado** CERT e de chooseInstall ID. Veja figura 12 por exemplo.**Figura 12: Instalando o certificado de identidade**
    Nota: Recomenda-se exportar o ponto confiável do certificado ID no ordewr para salvar o certificado e os pares de chaves emitidos. Isto permite que o administrador ASA importe o certificado e os pares de chaves a um ASA novo em caso do RMA ou da falha do hardware. Refira a exportação e a importação de pontos confiáveis para mais informação.**Nota: SALVAGUARDA do** clique a fim salvar a configuração na memória Flash.

Configuração de VPN de AnyConnect

Há duas opções a fim configurar os parâmetros VPN no ASDM. A primeira opção é usar o wizard VPN SSL. Esta é uma ferramenta fácil a usar-se para os usuários que são novos à configuração de VPN. A segunda opção é fazê-lo manualmente e atravessar cada opção. Este manual de configuração usa o método manual.

Nota: Há dois métodos para obter o cliente AC ao usuário:

1. Você pode transferir o cliente da site da Cisco na Web e instalá-lo em sua máquina.
2. O usuário pode alcançar o ASA através de um navegador da Web e o cliente pode ser transferido.

Nota: Por exemplo, https://asa.test.com. Este guia usa o segundo método. Uma vez que o cliente AC é instalado na máquina cliente permanentemente, você apenas lança o cliente AC do aplicativo.

Crie um pool do endereço IP de Um ou Mais Servidores Cisco ICM NT

Isto é opcional se você usa um outro método tal como o DHCP.

1. Escolha o **acesso remoto VPN > o acesso > a atribuição de endereço > os conjuntos de endereços da rede (cliente)**.
2. Clique em Add.
3. No indicador do IP pool adicionar, dê entrada com o nome do IP pool, começando e terminando o endereço IP de Um ou Mais Servidores Cisco ICM NT e escolha uma máscara de sub-rede. Consulte a Figura 13.**Figura 13: Adicionando o IP pool**
4. Escolha **está bem**.
5. Escolha a **política do acesso remoto VPN > do acesso > da atribuição de endereço > da atribuição da rede (cliente)**.

6. Selecione o método de atribuição apropriado do endereço IP de Um ou Mais Servidores Cisco ICM NT. Este guia usa as associações do endereço interno. Veja figura 14.**Figura 14: Método de atribuição do endereço IP de Um ou Mais Servidores Cisco ICM NT**
7. Clique em Apply.

Crie a política do grupo de túneis e do grupo

Agrupe a política

Nota: Se você não quer criar uma política nova, você pode usar a política construída padrão do em-grupo.

1. Escolha o **acesso remoto VPN - > acesso da rede (cliente) - > políticas do grupo**.
2. O clique **adiciona** e escolhe a **Política interna de grupo**.
3. No indicador da Política interna de grupo adicionar, dê entrada com o nome para a política do grupo na caixa de texto do nome. Veja figura 15.**Figura 15: Adicionando a Política interna de grupo** No tab geral, escolha o **cliente VPN SSL na** opção dos **protocolos de tunelamento**, a menos que você usar outros protocolos tais como os sem clientes SSL.Nos server secione, desmarcar a caixa de verificação **herdar** e incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do DNS e GANHE server. Incorpore o escopo de DHCP se aplicável.Nos server secione, deselect a caixa de verificação **herdar no** domínio padrão e incorpore o Domain Name apropriado.No tab geral, deselect a caixa de verificação **herdar na** seção do conjunto de endereços e adicionar o conjunto de endereços criado na etapa precedente. Se o youuse um outro método da atribuição do endereço IP de Um ou Mais Servidores Cisco ICM NT, sae deste para herdar e fazer a mudança apropriada.Todos guias de configuração restantes são deixados às configurações padrão.**Nota:** Há dois métodos para obter o cliente AC aos utilizadores finais. Um método é ir ao cisco.com e transferir o cliente AC. O segundo método é ter a transferência ASA o cliente ao usuário quando o usuário tenta conectar. Este exemplo mostra o último método.
4. Em seguida, escolha **avançado > ajustes do cliente VPN > do início de uma sessão SSL**. Veja figura 16.**Figura 16: Adicionando a Política interna de grupo** Deselect a caixa de seleção **herdar**.Escolha o ajuste apropriado do início de uma sessão do cargo que cabe seu ambiente.Escolha a seleção apropriada do início de uma sessão do cargo do padrão que cabe seu ambiente.Escolha **ESTÁ BEM**.

Relação e ajustes da imagem do grupo de túneis

Nota: Se você não quer criar um grupo novo, você pode usar o grupo do acessório do padrão.

1. Escolha o **acesso do acesso remoto VPN > da rede (cliente) > da conexão de VPN SSL perfil**.
2. Escolha **permitem o cliente de Cisco AnyConnect .....**
3. Uma caixa de diálogo aparece com a pergunta `você gostaria de designar uma imagem SVC?`
4. Escolha **sim**.
5. Se há já uma imagem, escolha a imagem usar-se com consultam o flash. Se a imagem não está disponível, escolha a **transferência de arquivo pela rede** e consulte para o arquivo no computador local. Veja figura 17. Os arquivos podem ser transferidos do cisco.com; há Windows, um MAC e um arquivo de Linux.**Figura 17: Adicionar a imagem do cliente VPN**

SSL
6. Permita em seguida **permitem o acesso**, **exigem o CERT do cliente** e **permitem** opcionalmente **DTL**. Veja figura 18.**Figura 18: Permitindo o acesso**
7. Clique em Apply.
8. Em seguida, crie um perfil de conexão/grupo de túneis. Escolha o **acesso do acesso remoto VPN > da rede (cliente) > da conexão de VPN SSL perfil**.
9. Nos perfis de conexão secione, clique **adicionam**.**Figura 19: Adicionando o perfil de conexão** Nomeie o grupo.Escolha o **certificado no** método de autenticação.Escolha a política do grupo criada previamente.Assegure-se de que o **cliente VPN SSL** esteja permitido.Deixe outras opções como o padrão.
10. Em seguida, chooseAdvanced **> autorização**. Veja figura 20**Figura 20: Autorização** Escolha o grupo AD-LDAP criado previamente.**Os usuários da** verificação **devem existir….para conectar.**Nos campos do mapeamento, não escolha o **UPN** para o preliminar e os **nenhuns** para secundário.
11. Escolha a seção **SSL VPN do** menu.
12. Na seção de pseudônimos da conexão, termine estas etapas:**Figura 21: Pseudônimos da conexão** Escolha **adicionam**.Inscreva o grupo aliás que você quer se usar.Assegure-se de que que **permitiu** é verificado. Consulte a Figura 21.
13. Clique em **OK**.

Nota: Salvaguarda do clique a fim salvar a configuração na memória Flash.

Regras de harmonização do certificado (se OCSP será usado)

1. Escolha o **acesso remoto VPN > avançou > certificado aos mapas do perfil da conexão de VPN SSL**. Veja figura 22.Escolha **adicionam no** certificado à seção dos mapas do perfil de conexão.Você pode manter o mapa existente como DefaultCertificateMap na seção do mapa ou criar um novo se você já usa mapas CERT para o IPsec.Mantenha a prioridade da regra.Sob o grupo traçado, saa como **-- Não traçado --**. Veja figura 22.**Figura 22: Adicionando a regra de harmonização do certificado**Clique em **OK**.
2. O clique **adiciona na** tabela inferior.
3. No critério de regra de harmonização do indicador do certificado adicionar, termine estas etapas:**Figura 23: Critério de regra de harmonização do certificado** Mantenha a coluna do campo **para sujeitar**.Mantenha a coluna componente ao **campo inteiro**.Mude o operador que a coluna **não iguala**.Na coluna de valor, incorpore duas aspas duplas **“”**.Clique a **aprovação** e **aplique-a**. Veja figura 23 por exemplo.

Configurar OCSP

A configuração de um OCSP pode variar e depende em cima do vendedor do que responde OCSP. Leia o manual do vendedor para mais informação.

Configurar o certificado do que responde OCSP

1. Obtenha um certificado auto-gerado do que responde OCSP.
2. Termine os procedimentos mencionados previamente e instale um certificado para o server OSCP.**Nota:** Certifique-se de que **não verifique Certificados para ver se há a revogação** está selecionado para o ponto confiável do certificado OCSP.

Configurar CA para usar OCSP

1. Escolha o **gerenciamento certificado > os certificados de CA do Acesso remoto VPN>**.
2. Destaque um OCSP a fim escolher CA configurar para usar OCSP.
3. O clique **edita**.
4. Assegure-se de que o **certificado da verificação para a revogação** esteja verificado.
5. Nos métodos da revogação secione, adicionar **OCSP**. Veja figura 24.**Verificação da revogação OCSP**
6. Assegure **consideram o certificado válido… não pode ser recuperado** é desmarcado se você quer seguir a verificação restrita OCSP.

Nota: Configurar/edite todo o server de CA que usa OCSP para a revogação.

Configurar regras OCSP

Nota: Verifique que uma política de harmonização do grupo do certificado está criada e o que responde OCSP está configurado antes que você termine estas etapas.

Nota: Em aplicações algum OCSP, um registro DNS A e PTR pode ser precisado para o ASA. Esta verificação é feita a fim verificar que o ASA é de um local .mil.

1. Escolha o **gerenciamento certificado do Acesso remoto VPN> > os certificados de CA 2.**
2. Destaque um OCSP a fim escolher CA configurar para usar OCSP.
3. Escolha **editam**.
4. Clique a aba da **regra OCSP**.
5. Clique em Add.
6. No indicador da regra adicionar OCSP, termine estas etapas. Veja figura 25.**Figura 25: Adicionando regras OCSP** Na opção do mapa do certificado, escolha **DefaultCertificateMap** ou um mapa criado previamente.Na opção do certificado, escolha o **que responde OCSP**.Na opção de deslocamento predeterminado, incorpore o **10.**Na opção URL, entre no endereço IP de Um ou Mais Servidores Cisco ICM NT ou no hostname do que responde OCSP. Se você usa o hostname, certifique-se que o servidor DNS está configurado no ASA.Clique a **aprovação**.Clique em Apply.

Configuração de cliente de Cisco AnyConnect

Esta seção cobre a configuração do Cisco AnyConnect VPN Client.

Suposições — O aplicativo do Cisco AnyConnect VPN Client e do middleware é instalado já no host PC. O ouro e ActivClient de ActivCard foram testados.

Nota: Este guia usa o método grupo-URL para o cliente inicial AC instala somente. Uma vez que o cliente AC é instalado, você lança o aplicativo AC apenas como o cliente de IPSec.

Nota: O certificate chain do DoD precisa de ser instalado na máquina local. Verifique com o POC PKI a fim obter os Certificados/arquivo de lote.

Nota: O direcionador do leitor de cartão para o MAC OSX é já instalado e compatível com a versão de OS atual que você usa.

Transferindo o Cisco AnyConnect VPN Client – Mac OS X

1. Lance uma sessão da web ao ASA com o safari. O endereço deve estar no formato de https://Outside-Interface. Por exemplo, https://172.18.120.225.
2. Uma janela pop-up pede para verificar o certificado do ASA. Clique em **Continuar**.
3. Uma outra janela pop-up aparece a fim destravar o keychain CAC. Entre em seu número Pin. Veja figura 31.**Figura 31: Incorpore o PIN**
4. Depois que o página da web do VPN-serviço SSL se publica, o clique **continua**.
5. Depois que você destrava o keychain, o navegador alerta-o se você confia o certificado do ASA. **Confiança do** clique.
6. Incorpore a senha root a fim destravar o keychain para estabelecer a conexão segura, e clique então a **aprovação**.
7. Escolha o certificado usar-se para a authenticação do cliente, e clique então a **aprovação**.
8. O navegador pede então a raiz/senha do usuário a fim permitir transferir de clientes de AnyConnect.
9. Se autenticado, o cliente de AnyConnect começa transferir. Consulte a Figura 32.**Figura 32: Transferência de AnyConnect**
10. Depois que o aplicativo é transferido, o navegador alerta-o aceitar o certificado ASA. O clique **aceita**.
11. A conexão é estabelecida. Figura 33.**Figura 33:AnyConnect conectada**

Cisco AnyConnect VPN Client do começo – Mac OS X

Do inventor **— Aplicativos > Cisco AnyConnect VPN Client**

Nota: Veja o apêndice E para a configuração de perfil opcional do cliente de AnyConnect.

Nova conexão

O indicador AC aparece. Veja figura 37.

Figura 37: Conexão de VPN nova

1. Escolha o host apropriado se o AC não tenta automaticamente a conexão.
2. Incorpore seu PIN quando alertado. Veja figura 38.**Figura 38: Incorpore o PIN**

Comece o Acesso remoto

1. Escolha o grupo e hospede-o a qual você quer conectar.
2. Desde que os Certificados são usados, escolha **conectam** a fim estabelecer o VPN. Veja figura 39.**Nota:** Desde que a conexão usa Certificados, não há nenhuma necessidade de incorporar um nome de usuário e senha.**Figura 39:** Conectando **Nota:** Veja o apêndice E para a configuração de perfil opcional do cliente de AnyConnect.

Apêndice A – Mapeamento LDAP e DAP

Em ASA/PIX libere 7.1(x) e mais atrasado, uma característica chamada mapeamento LDAP foi introduzida. Esta é uma característica poderosa que forneça um mapeamento entre um atributo

de Cisco e objetos LDAP/atributo, que negue a necessidade para a mudança do esquema LDAP. Para a aplicação da autenticação CAC, isto pode apoiar o reforço de política adicional na conexão de acesso remoto. Estes são exemplos do mapeamento LDAP. Esteja ciente que você precisa direitos do administrador a fim fazer mudanças no server AD/LDAP. No software ASA 8.x, a característica da política do acesso dinâmico (DAP) foi introduzida. O DAP pode trabalhar conjuntamente com o CAC para olhar grupos múltiplos AD assim como para empurrar e assim por diante políticas, ACL.

Cenário 1: Aplicação do diretório ativo usando o discado da permissão de acesso remoto – Permita/negue o acesso

Este exemplo traça o msNPAllowDailin do atributo AD ao protocolo do atributo cVPN3000-Tunneling- de Cisco.

- O valor de atributo AD: VERDADEIRO = reserve; FALSO = negue
- Valor de atributo de Cisco: 1 = FALSO, 4 (IPsec) ou 20 (IPSEC 4 + 16 o WebVPN) = RETIFICA,

Para a condição ALLOW, você traça:

- RETIFIQUE = 20

Para a condição do discado DENY, você traça:

- = 1 FALSO

Nota: Certifique-se de que VERDADEIRO e FALSO esteja em todos os tampões. Refira configurar um servidor interno para a autorização de usuário da ferramenta de segurança para mais informação.

Instalação do diretório ativo

1. No servidor ative directory, **Iniciar > Executar do** clique.
2. Na caixa de texto aberta, datilografe **dsa.msc a seguir** clique a aprovação**. Isto** liga o console de gerenciamento do diretório ativo.
3. No console de gerenciamento do diretório ativo, clique o sinal positivo a fim expandir os usuários e os computadores de diretório ativo.
4. Clique o sinal positivo a fim expandir o Domain Name.
5. Se você tem um OU criado para seus usuários, expanda o OU a fim ver todos os usuários; se você tem todos os usuários atribuídos na pasta de usuários, expanda esse dobrador a fim vê-los. Veja a figura A1.**Figura A1: Console de gerenciamento do diretório ativo**
6. Clique duas vezes no usuário que você quer editar.Clique sobre o guia de discagem de entrada na página das propriedades de usuário e clique-o sobre **reservam** ou **negam**. Veja a figura A2.**Figura A2: Propriedades de usuário**
7. Clique então a **aprovação**.

Configuração ASA

1. No ASDM, escolha o **Acesso remoto VPN> AAA Setup > mapa do atributo LDAP**.
2. Clique em Add.
3. No indicador do mapa do atributo adicionar LDAP, termine estas etapas. Veja a figura

A3.**Figura A3: Adicionando o mapa do atributo LDAP** Dê entrada com um nome na caixa de texto do nome.Na aba do nome de mapa, datilografe o **msNPAllowDialin na** caixa de texto do nome do cliente.Na aba do nome de mapa, escolha **protocolos de tunelamento na** opção da gota-para baixo no nome de Cisco.Clique em Add.Escolha a aba do **valor do mapa**.Clique em Add.No indicador do valor do mapa do atributo LDAP adicionar, datilografe **VERDADEIRO na** caixa de texto do nome do cliente e no tipo **20 na** caixa de texto do valor de Cisco.Clique em Add.Datilografe **FALSO na** caixa de texto e no tipo-1 do nome do cliente na caixa de texto do valor de Cisco. Veja a figura A4.Clique a **aprovação**.Clique a **aprovação**.Clique em Apply.A configuração deve olhar como a figura A5.**Figura A5: Configuração de mapa do atributo LDAP**

4. Escolha o **Acesso remoto VPN> AAA Setup > Grupos de servidores AAA**. Veja a figura A6.**Figura A6: Grupos de servidores AAA**
5. Clique sobre o grupo de servidor que você quer editar. Nos server na seção de grupo selecionada, escolha o endereço IP do servidor ou o hostname, e clique-os então **editam**.
6. Em edite o indicador do servidor AAA, na caixa de texto do mapa do atributo LDAP, escolhem o mapa do atributo LDAP criado no menu suspenso. Veja a figura A7**Figura A7: Adicionando o mapa do atributo LDAP**
7. **Aprovação do** clique.

Nota: Gire sobre a eliminação de erros LDAP quando você testar a fim verificar se o emperramento LDAP e o mapeamento do atributo trabalham corretamente. Veja o C do apêndice para comandos de Troubleshooting.

Cenário 2: A aplicação do diretório ativo usando a membrasia do clube para reservar/nega o acesso

Este exemplo usa o memberOf do atributo LDAP para traçar ao atributo do protocolo de tunelamento a fim estabelecer uma membrasia do clube como uma circunstância. Para que esta política trabalhe, você deve ter estas circunstâncias:

- Use um grupo que já exista ou crie um grupo novo para que os usuários ASA VPN sejam um membro para de condições ALLOW.
- Use um grupo que já exista ou crie um grupo novo para que não os usuários ASA sejam um membro para de condições DENY.
- Certifique-se verificar dentro o visor LDAP que você tenha o DN direito para o grupo. Consulte o Apêndice D. Se o DN é errado, o mapeamento não trabalha corretamente.

Nota: Esteja ciente que o ASA pode somente ler a primeira corda do atributo do memeberOf nesta liberação. Certifique-se de que o grupo novo criado está na parte superior da lista. A outra opção é pôr um caractere especial na frente do nome porque o AD olha caracteres especiais primeiramente. A fim trabalhar em torno desta advertência, use o DAP no software 8.x para olhar grupos múltiplos.

Nota: Certifique-se que um usuário é parte do grupo da negação ou pelo menos outro um grupo de modo que o memberOf seja enviado sempre para trás ao ASA. Você não tem que especificar o FALSO nega a circunstância mas o melhor prática é fazer assim. Se o nome de grupo existente ou o nome do grupo contêm um espaço, incorpore o atributo desse modo:

```
CN=Backup Operators,CN=Builtin,DC=ggsgseclab,DC=org
```

Nota: O DAP permite que o ASA olhe grupos múltiplos no atributo do memberOf e na autorização baixa fora dos grupos. Veja a seção DAP.

TRAÇO

- O valor de atributo AD:memberOf CN=ASAUsers, cn=Users, DC=ggsgseclab, DC=orgmemberOf CN=TelnetClients, cn=Users, DC=labrat, dc=com
- Valor de atributo de Cisco: 1 = FALSO, 20 = RETIFICA,

Para a condição **ALLOW**, você traça:

- memberOf CN=ASAUsers, cn=Users, DC=ggsgseclab, DC=org= 20

Para a condição **DENY**, você traça:

- memberOf CN=TelnetClients, cn=Users, DC=ggsgseclab, DC=org = 1

Nota: Na liberação futura, há um atributo de Cisco a fim permitir e negar a conexão. Refira configurar um servidor interno para a autorização de usuário da ferramenta de segurança para obter mais informações sobre dos atributos de Cisco.

Instalação do diretório ativo

1. No servidor ative directory, escolha o **Iniciar > Executar**.
2. Na caixa de texto aberta, datilografe **dsa.msc, e** clique então a aprovação**. Isto** liga o console de gerenciamento do diretório ativo.
3. No console de gerenciamento do diretório ativo, clique o sinal positivo a fim expandir os usuários e os computadores de diretório ativo. Veja a figura A8**Figura A8: Grupos do diretório ativo**
4. Clique o sinal positivo a fim expandir o Domain Name.
5. Clicar com o botão direito na **pasta de usuários** e escolha **novo > grupo**.
6. Dê entrada com um nome do grupo. Por exemplo: ASAUsers.
7. **Aprovação do** clique.
8. Clique sobre a **pasta de usuários**, e fazer duplo clique então no grupo que você apenas criou.
9. Escolha a aba dos **membros**, e clique-a então **adicionam**.
10. Datilografe o nome do usuário que você quer adicionar, e clique então a **aprovação**.

Configuração ASA

1. No ASDM, escolha o **acesso remoto VPN > o AAA Setup > mapa do atributo LDAP**.
2. Clique em Add.
3. No indicador do mapa do atributo adicionar LDAP, termine estas etapas. Veja a figura A3.Dê entrada com um nome na caixa de texto do nome.Na aba do nome de mapa, datilografe o **memberOf na** caixa de texto C. do nome do cliente.Na aba do nome de mapa, escolha **protocolos de tunelamento na** opção da gota-para baixo no nome de Cisco.Escolha **adicionam**.Clique a aba do **valor do mapa**.Escolha **adicionam**.No indicador do valor do mapa do atributo LDAP adicionar, datilografe **CN=ASAUsers, cn=Users, DC=ggsgseclab, DC=org na** caixa de texto do nome do cliente e no tipo **20 na** caixa de texto do valor de Cisco.Clique em Add.Datilografe **CN=TelnetClients, cn=Users, DC=ggsgseclab, DC=org na** caixa de texto e no tipo-1 do nome do cliente na caixa de texto do valor de Cisco. Veja a figura A4.Clique a **aprovação**.Clique a **aprovação**.Clique em Apply.A configuração deve olhar como a figura A9.**Figura mapa do atributo A9 LDAP**
4. Escolha o **Acesso remoto VPN> AAA Setup > Grupos de servidores AAA**.

5. Clique sobre o grupo de servidor que você quer editar. Nos server na seção de grupo selecionada, selecione o endereço IP do servidor ou o hostname, e clique-os então **editam**
6. Em edite o indicador do servidor AAA, na caixa de texto do mapa do atributo LDAP, selecionam o mapa do atributo LDAP criado no menu suspenso.
7. Clique a **aprovação**.

Nota: Gire sobre a eliminação de erros LDAP quando você testar a fim verificar que emperramento LDAP e para atribuir mapeamentos trabalha corretamente. Veja o C do apêndice para comandos de Troubleshooting.

Cenário 3: Políticas do acesso dinâmico para atributos múltiplos do memberOf

Este exemplo usa o DAP para olhar atributos múltiplos do memberOf a fim permitir o acesso baseado fora da membrasia do clube do diretório ativo. Antes de 8.x, o ASA leu somente o primeiro atributo do memberOf. Com 8.x e mais tarde, o ASA pode olhar todos os atributos do memberOf.

- Use um grupo que já exista ou crie um grupo novo (ou grupos múltiplos) para que os usuários ASA VPN sejam um membro para de condições ALLOW.
- Use um grupo que já exista ou crie um grupo novo para que não os usuários ASA sejam um membro para de condições DENY.
- Certifique-se verificar dentro o visor LDAP que você tenha o DN direito para o grupo. Consulte o Apêndice D. Se o DN é errado, o mapeamento não trabalha corretamente.

Configuração ASA

1. No ASDM, escolha **políticas do acesso > do acesso dinâmico da rede do Acesso remoto VPN> (cliente)**.
2. Clique em Add.
3. Na política do acesso dinâmico adicionar, termine estas etapas:Dê entrada com um nome na caixa de texto B. do nome.Na seção de prioridade, incorpore **1**, ou um número maior de 0.Nos critérios de seleção, o clique **adiciona**.No atributo adicionar AAA, escolha o **LDAP**.Na seção do atributo ID, incorpore o **memberOf**.Na seção do valor, escolha **=** e dê entrada com o nome do grupo AD. Repita esta etapa para cada grupo que você quer prover. Veja a figura A10.**Figure o mapa do atributo A10 AAA**Clique em **OK**.Na política de acesso atribui a seção, chooseContinue. Veja a figura A11.**A figura A11 adiciona a política dinâmica**
4. No ASDM, escolha **políticas do acesso > do acesso dinâmico da rede do Acesso remoto VPN> (cliente)**.
5. Escolha a **política de acesso do padrão** e escolha-a **editam**.
6. A ação padrão deve ser ajustada **para terminar**. Veja a figura A12.**A figura A12 edita a política dinâmica**
7. **Aprovação do** clique.

Nota: Se **Terminate** não é selecionada, está permitido você dentro mesmo se não em todos os grupos porque o padrão é continuar.

Apêndice B – Configuração de CLI ASA

ASA 5510

```
ciscoasa#show running-config : Saved : ASA Version
8.0(2) ! hostname asa80 domain-name army.mil enable
password 8Ry2YjIyt7RRXU24 encrypted names ! interface
GigabitEthernet0/0 nameif outside security-level 0 ip
address x.x.x.x 255.255.255.128 ! interface
GigabitEthernet0/1 nameif inside security-level 100 no
ip address ! boot system disk0:/asa802-k8.bin ftp mode
passive dns server-group DefaultDNS domain-name army.mil
! --------------ACL's-----------------------------------
-------------- access-list out extended permit ip any
any ------------------------------------------------
---------------- pager lines 24 logging console
debugging mtu outside 1500 ! ---------------VPN Pool----
---------------------------------------- ip local pool
CAC-USERS 192.168.1.1-192.168.1.254 mask 255.255.255.0 -
------------------------------------------------------
----------- ! no failover icmp unreachable rate-limit 1
burst-size 1 asdm image disk0:/asdm-602.bin no asdm
history enable arp timeout 14400 access-group out in
interface outside route outside 0.0.0.0 0.0.0.0
172.18.120.129 1 timeout xlate 3:00:00 timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media
0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute ! ----------------------
---LDAP Maps & DAP--------------------------- ldap
attribute-map memberOf map-name memberOf Tunneling-
Protocols March 11, 2008 ASA – CAC Authentication for
AnyConnect VPN Access Company Confidential. A printed
copy of this document is considered uncontrolled. 49
map-value memberOf
CN=_ASAUsers,CN=Users,DC=ggsgseclab,DC=org 20 ldap
attribute-map msNPAllowDialin map-name msNPAllowDialin
Tunneling-Protocols map-value msNPAllowDialin FALSE 1
map-value msNPAllowDialin TRUE 20 dynamic-access-policy-
record CAC-USERS description "Multi-Group Membership
Check" priority 1 dynamic-access-policy-record
DfltAccessPolicy action terminate ----------------------
------------------------------------------- ! -------
-------------LDAP Server--------------------------------
----- aaa-server AD-LDAP protocol ldap aaa-server AD-
LDAP (outside) host 172.18.120.160 ldap-base-dn
CN=Users,DC=ggsgseclab,DC=org ldap-scope onelevel ldap-
naming-attribute userPrincipalName ldap-login-password *
ldap-login-dn
CN=Administrator,CN=Users,DC=ggsgseclab,DC=org ---------
------------------------------------------------------
--- ! aaa authentication http console LOCAL http server
enable 445 http 0.0.0.0 0.0.0.0 outside no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart ! --------
--------CA Trustpoints-----------------------------------
---- crypto ca trustpoint ASDM_TrustPoint0 revocation-
check ocsp enrollment terminal keypair DoD-1024 match
certificate DefaultCertificateMap override ocsp
trustpoint ASDM_TrustPoint5 10 url http://ocsp.disa.mil
crl configure crypto ca trustpoint ASDM_TrustPoint1
revocation-check ocsp enrollment terminal fqdn asa80
subject-name CN=asa80,OU=PKI,OU=DoD,O=U.S.
Government,C=US keypair DoD-1024 match certificate
DefaultCertificateMap override ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil no client-
types crl configure crypto ca trustpoint
```

```
ASDM_TrustPoint2 revocation-check ocsp enrollment
terminal keypair DoD-2048 match certificate
DefaultCertificateMap override ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil no client-
types crl configure crypto ca trustpoint
ASDM_TrustPoint3 revocation-check ocsp none enrollment
terminal crl configure ! ------------------Certificate
Map----------------------------- crypto ca certificate
map DefaultCertificateMap 10 subject-name ne "" --------
------------CA Certificates (Partial Cert is Shown)-----
------- crypto ca certificate chain ASDM_TrustPoint0
certificate ca 37 3082044c 30820334 a0030201 02020137
300d0609 2a864886 f70d0101 05050030 60310b30 09060355
04061302 55533118 30160603 55040a13 0f552e53 2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c
300a0603 55040b13 03504b49 311b3019 06035504 03131244
6f44204a 49544320 526f6f74 crypto ca certificate chain
ASDM_TrustPoint1 certificate 319e 30820411 3082037a
a0030201 02020231 9e300d06 092a8648 86f70d01 01050500
305c310b 30090603 55040613 02555331 18301606 0355040a
130f552e 532e2047 6f766572 6e6d656e 74310c30 0a060355
040b1303 446f4431 0c300a06 0355040b crypto ca
certificate chain ASDM_TrustPoint2 certificate ca 37
3082044c 30820334 a0030201 02020137 300d0609 2a864886
f70d0101 05050030 60310b30 09060355 04061302 55533118
30160603 55040a13 0f552e53 2e20476f 7665726e 6d656e74
310c300a 06035504 0b130344 6f44310c 300a0603 55040b13
f766e045 f15ddb43 9549d1e9 a0ea6814 b64bcece 089e1b6e
1be959a5 6fc20a76 crypto ca certificate chain
ASDM_TrustPoint3 certificate ca 05 30820370 30820258
a0030201 02020105 300d0609 2a864886 f70d0101 05050030
5b310b30 09060355 04061302 55533118 30160603 55040a13
0f552e53 2e20476f 7665726e 6d656e74 310c300a 06035504
0b130344 6f44310c 300a0603 55040b13 03504b49 31163014
06035504 03130d44 6f442052 6f6f7420 43412032 301e170d
30343132 31333135 30303130 5a170d32 39313230 35313530
3031305a 305b310b 30090603 55040613 02555331 18301606
0355040a 130f552e 532e2047 6f766572 6e6d656e 74310c30
0a060355 040b1303 446f4431 0c300a06 0355040b 1303504b
49311630 14060355 0403130d 446f4420 526f6f74 20434120
32308201 crypto ca certificate chain ASDM_TrustPoint4
certificate ca 04 30820267 308201d0 a0030201 02020104
300d0609 2a864886 f70d0101 05050030 61310b30 09060355
04061302 55533118 30160603 55040a13 0f552e53 2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c
300a0603 55040b13 03504b49 311c301a 06035504 03131344
6f442043 4c415353 20332052 6f6f7420 ! ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
! -------------------------SSL/WEBVPN------------------
----------------- ssl certificate-authentication
interface outside port 443 webvpn enable outside svc
image disk0:/anyconnect-win-2.0.0343-k9.pkg 1 svc enable
tunnel-group-list enable ------------------------------
------------------------------------ ------------------
-----VPN Group/Tunnel Policy-------------------- group-
policy CAC-USERS internal ggroup-policy AC-USERS
internal group-policy AC-USERS attributes vpn-tunnel-
```

```
protocol svc address-pools value CAC-USERS webvpn svc
ask none default svc tunnel-group AC-USERS type remote-
access tunnel-group AC-USERS general-attributes
authorization-server-group AD-LDAP default-group-policy
AC-USERS authorization-required authorization-dn-
attributes UPN tunnel-group AC-USERS webvpn-attributes
authentication certificate group-alias AC-USERS enable
tunnel-group-map enable rules no tunnel-group-map enable
ou no tunnel-group-map enable ike-id no tunnel-group-map
enable peer-ip ----------------------------------------
-------------------------- prompt hostname context
```

Troubleshooting do apêndice c

Pesquisando defeitos o AAA e o LDAP

- **debugar o ldap 255** — Trocas dos indicadores LDAP
- **debugar aaa 10 comum** — Trocas dos indicadores AAA

Exemplo 1: Conexão permitida com o mapeamento correto do atributo

Este exemplo mostra que a saída de **debuga o ldap** e **debuga o aaa comum** durante uma conexão bem sucedida com a encenação 2 mostrada no apêndice A.

Figura C1: debugar o LDAP e debugar a saída comum aaa – mapeamento correto

```
AAA API: In aaa_open
AAA session opened: handle = 39
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type
0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
-------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[78] Session Start
[78] New request Session, context 0x26f1c44, reqType = 0
[78] Fiber started
[78] Creating LDAP context with uri=ldap://
172.18.120.160:389
[78] Binding as administrator
[78] Performing Simple authentication for Administrator
to
172.18.120.160
[78] Connect to LDAP server: ldap:// 172.18.120.160,
status =
Successful
[78] LDAP Search:
Base DN = [CN=Users,DC=ggsgseclab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
```

```
[78] Retrieved Attributes:
[78] objectClass: value = top
[78] objectClass: value = person
[78] objectClass: value = organizationalPerson
[78] objectClass: value = user
[78] cn: value = Ethan Hunt
[78] sn: value = Hunt
[78] userCertificate: value =
0..50........../........60...*.H........0@1.0.....&...,d
....com1.0.....
&...,d...
[78] userCertificate: value =
0..'0........../..t.....50...*.H........0@1.0.....&...,d
....com1.0.....
&...,d...
[78] givenName: value = Ethan
[78] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[78] instanceType: value = 4
[78] whenCreated: value = 20060613151033.0Z
[78] whenChanged: value = 20060622185924.0Z
[78] displayName: value = Ethan Hunt
[78] uSNCreated: value = 14050
[78] memberOf: value =
CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[78] mapped to cVPN3000-Tunneling-Protocols: value = 20
[78] uSNChanged: value = 14855
[78] name: value = Ethan Hunt
[78] objectGUID: value = ..9...NJ..GU..z.
[78] userAccountControl: value = 66048
[78] badPwdCount: value = 0
[78] codePage: value = 0
[78] countryCode: value = 0
[78] badPasswordTime: value = 127954717631875000
[78] lastLogoff: value = 0
[78] lastLogon: value = 127954849209218750
[78] pwdLastSet: value = 127946850340781250
[78] primaryGroupID: value = 513
[78] objectSid: value = ................q......mY...
[78] accountExpires: value = 9223372036854775807
[78] logonCount: value = 25
[78] sAMAccountName: value = 1234567890
[78] sAMAccountType: value = 805306368
[78] userPrincipalName: value = 1234567890@mil
[78] objectCategory: value =
[78] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
[78] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[78] Session End
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE,
auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-
LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state =
```

```
IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(CAC-USERS)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp:
GROUP_POLICY_DB)
-------------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
User: CAC-USER
Pasw:
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a870b4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY,
auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-
LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user
1234567890@mil
AAA FSM: In AAA_Callback
user attributes:
1 Tunnelling-Protocol(4107) 20 20
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunnelling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "ggsgseclab.org"
5 List of address pools to assign addresses from(4313)
10
"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type
3
In aaai_close_session (39)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
CAC-Test#
```

Exemplo 2: Conexão permitida com o mapeamento desconfigurado do atributo de Cisco

Este exemplo mostra que a saída de **debuga o ldap** e **debuga o aaa comum** durante uma conexão permitida com a encenação 2 mostrada no apêndice A.

Figura C2: debugar o LDAP e debugar a saída comum aaa – mapeamento incorreto

```
AAA API: In aaa_open
AAA session opened: handle = 41
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type
0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
-------------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[82] Session Start
[82] New request Session, context 0x26f1c44, reqType = 0
[82] Fiber started
[82] Creating LDAP context with
uri=ldap://172.18.120.160:389
[82] Binding as administrator
[82] Performing Simple authentication for Administrator
to
172.18.120.160
[82] Connect to LDAP server: ldap:// 172.18.120.160:389,
status =
Successful
[82] LDAP Search:
Base DN = [CN=Users,DC=ggsgseclab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
[82] Retrieved Attributes:
[82] objectClass: value = top
[82] objectClass: value = person
[82] objectClass: value = organizationalPerson
[82] objectClass: value = user
[82] cn: value = Ethan Hunt
[82] sn: value = Hunt
[82] userCertificate: value =
0..50........../........60...*.H........0@1.0.....&...,d
....com1.0.....
&...,d...
[82] userCertificate: value =
0..'0........../..t.....50...*.H........0@1.0.....&...,d
....com1.0.....
&...,d...
[82] givenName: value = Ethan
[82] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[82] instanceType: value = 4
[82] whenCreated: value = 20060613151033.0Z
[82] whenChanged: value = 20060622185924.0Z
[82] displayName: value = Ethan Hunt
[82] uSNCreated: value = 14050
[82] memberOf: value =
CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[82] mapped to cVPN3000-Tunneling-Protocols: value =
CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[82] uSNChanged: value = 14855
[82] name: value = Ethan Hunt
```

```
[82] objectGUID: value = ..9...NJ..GU..z.
[82] userAccountControl: value = 66048
[82] badPwdCount: value = 0
[82] codePage: value = 0
[82] countryCode: value = 0
[82] badPasswordTime: value = 127954717631875000
[82] lastLogoff: value = 0
[82] lastLogon: value = 127954849209218750
[82] pwdLastSet: value = 127946850340781250
[82] primaryGroupID: value = 513
[82] objectSid: value = ................q......mY...
[82] accountExpires: value = 9223372036854775807
[82] logonCount: value = 25
[82] sAMAccountName: value = 1234567890
[82] sAMAccountType: value = 805306368
[82] userPrincipalName: value = 1234567890@mil
[82] objectCategory: value =
CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=or
g
[82] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
[82] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[82] Session End
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE,
auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-
LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state =
IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(USAFE)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp:
GROUP_POLICY_DB)
-------------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
User: CAC-USERS
Pasw:
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a870b4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type
1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY,
```

```
auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-
LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user
1234567890@mil
AAA FSM: In AAA_Callback
user attributes:
1 Tunnelling-Protocol(4107) 20 0
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunnelling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "ggsgseclab.org"
5 List of address pools to assign addresses from(4313)
10
"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type
3
In aaai_close_session (41)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
```

Pesquisando defeitos o DAP

- **debugar erros do dap** — Erros dos indicadores DAP
- **debugar o traço do dap** — Traço da função dos indicadores DAP

Exemplo 1: Conexão permitida com o DAP

Este exemplo mostra que a saída de **debuga erros do dap** e **debuga o traço do dap** durante uma conexão bem sucedida com a encenação 3 mostrada no apêndice A. Atributos múltiplos do memberOf da observação. Você pode pertencer aos _ASAUsers e o VPNUsers ou o tp um ou outro grupo, que depende da configuração ASA.

Figura C3: debugar o DAP

```
#debug dap errors debug dap errors enabled at level 1
#debug dap trace debug dap trace enabled at level 1 #
The DAP policy contains the following attributes for
user: 1241879298@mil ----------------------------------
---------------------------------- --- 1: action =
continue DAP_TRACE: DAP_open: C8EEFA10 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.2 = person DAP_TRACE: Username:
1241879298@mil, aaa.ldap.objectClass.3 =
organizationalPerson DAP_TRACE: Username:
1241879298@mil, aaa.ldap.objectClass.4 = user DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.cn = 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName
= 1241879298 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=ggsgseclab,DC=org DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.whenCreated = 20070626163734.0Z DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.whenChanged =
20070718151143.0Z DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.displayName = 1241879298 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.uSNCreated = 33691 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.memberOf.1 = VPNUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.2
= _ASAUsers DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.uSNChanged = 53274 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.department = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name =
1241879298 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectGUID = ....+..F.."5.... DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.userAccountControl =
328192 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.badPwdCount = 0 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.codePage = 0 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.badPasswordTime = 0 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.lastLogoff = 0 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.lastLogon = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet
= 128273494546718750 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.primaryGroupID = 513 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.userParameters = m:
d. DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectSid = .. DAP_TRACE: Username:
1241879298@mil, aaa.ldap.accountExpires =
9223372036854775807 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.logonCount = 0 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.sAMAccountName = 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.sAMAccountType = 805306368 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.userPrincipalName =
1241879298@mil DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectCategory =
CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=or
g DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.msNPAllowDialin = TRUE DAP_TRACE: Username:
1241879298@mil, aaa.cisco.username = 1241879298@mil
DAP_TRACE: Username: 1241879298@mil,
aaa.cisco.tunnelgroup = CAC-USERS DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] =
"top"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user"; DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"]
= "1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeN
ame"] = "NETADMIN"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["givenName"] =
"1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=ggsgseclab,DC=org";
```

```
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["1"] =
"VPNUsers"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["2"] =
"_ASAUsers"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"]
= "NETADMIN"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"]
contains binary data DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] =
"0"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] =
"0"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"]
= "0"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] =
"513"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userParameters"]
contains binary data DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains
binary data DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=o
rg"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] =
"TRUE"; DAP_TRACE:
dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil"; DAP_TRACE:
dap_add_to_lua_tree:aaa["cisco"]["tunnelgroup"] =
"CACUSERS"; DAP_TRACE:
dap_add_to_lua_tree:endpoint["application"]["clienttype"
] = "IPSec"; DAP_TRACE: Username: 1241879298@mil,
Selected DAPs: CAC-USERS DAP_TRACE: dap_request: memory
usage = 33% DAP_TRACE: dap_process_selected_daps:
```

```
selected 1 records DAP_TRACE: Username: 1241879298@mil,
dap_aggregate_attr: rec_count = 1 DAP_TRACE: Username:
1241879298@mil, DAP_close: C8EEFA10 d.
```

Exemplo 2: Conexão negada com o DAP

O exemplo de Thia mostra que a saída de **debuga erros do dap** e **debuga o traço do dap** durante uma conexão mal sucedida com a encenação 3 mostrada no apêndice A.

Figura C4: debugar o DAP

```
#debug dap errors debug dap errors enabled at level 1
#debug dap trace debug dap trace enabled at level 1 #
The DAP policy contains the following attributes for
user: 1241879298@mil ----------------------------------
---------------------------------- --- 1: action =
terminate DAP_TRACE: DAP_open: C91154E8 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectClass.2 = person DAP_TRACE: Username:
1241879298@mil, aaa.ldap.objectClass.3 =
organizationalPerson DAP_TRACE: Username:
1241879298@mil, aaa.ldap.objectClass.4 = user DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.cn = 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName
= 1241879298 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=ggsgseclab,DC=org DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.whenCreated = 20070626163734.0Z DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.whenChanged =
20070718151143.0Z DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.displayName = 1241879298 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.uSNCreated = 33691 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.memberOf = DnsAdmins
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged
= 53274 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.department = NETADMIN DAP_TRACE: Username:
1241879298@mil, aaa.ldap.name = 1241879298 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.objectGUID =
....+..F.."5.... DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userAccountControl = 328192 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage =
0 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.countryCode = 0 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.badPasswordTime = 0 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.lastLogoff = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon
= 0 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.pwdLastSet = 128273494546718750 DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.userParameters = m: d. DAP_TRACE: Username:
1241879298@mil, aaa.ldap.objectSid = .. DAP_TRACE:
Username: 1241879298@mil, aaa.ldap.accountExpires =
9223372036854775807 DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.logonCount = 0 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.sAMAccountName = 1241879298
```

```
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.sAMAccountType = 805306368 DAP_TRACE: Username:
1241879298@mil, aaa.ldap.userPrincipalName =
1241879298@mil DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.objectCategory =
CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=or
g DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.msNPAllowDialin = TRUE DAP_TRACE: Username:
1241879298@mil, aaa.cisco.username = 1241879298@mil
DAP_TRACE: Username: 1241879298@mil,
aaa.cisco.tunnelgroup = CAC-USERS DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] =
"top"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user"; DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"]
= "1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeN
ame"] = "NETADMIN"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["givenName"] =
"1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=ggsgseclab,DC=org";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"] =
"DnsAdmins"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"]
= "NETADMIN"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"]
contains binary data DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] =
"0"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] =
"0"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"]
= "0"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] =
"513"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userParameters"]
contains binary data DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains
binary data DAP_TRACE:
```

```
dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=o
rg"; DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] =
"TRUE"; DAP_TRACE:
dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil"; DAP_TRACE: Username: 1241879298@mil,
Selected DAPs: DAP_TRACE: dap_request: memory usage =
33% DAP_TRACE: dap_process_selected_daps: selected 0
records DAP_TRACE: Username: 1241879298@mil,
dap_aggregate_attr: rec_count = 1
```

Pesquisando defeitos o Certificate Authority/OCSP

- **debug crypto ca 3**
- No modo de configuração **— a classe de registro Ca consola (ou buffer) a eliminação de erros**

Estes exemplos mostram uma validação certificada bem sucedida com o que responde OCSP e uma política de harmonização falhada do grupo do certificado.

A figura C3 mostra o resultado do debug que tem um certificado validado e uma política de harmonização de trabalho do grupo do certificado.

A figura C4 mostra o resultado do debug de uma política de harmonização do grupo desconfigurado do certificado.

A figura C5 mostra o resultado do debug de um usuário com um certificado revogado.

Figura C5: Eliminação de erros OCSP – validação certificada bem sucedida

```
CRYPTO_PKI: Found a suitable authenticated trustpoint
ASDM_TrustPoint11.
CRYPTO_PKI: Allocated OCSP data handle 0xca2d27b8
CRYPTO_PKI: Certificate validation: Successful, status:
0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: status = 0: poll revocation status
CRYPTO_PKI: Attempting to find OCSP override for peer
cert: serial
number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
CRYPTO_PKI: Processing map rules for SSL.
CRYPTO_PKI: Processing map SSL sequence 20...
CRYPTO_PKI: Match of subject-name field to map PASSED.
Peer cert field:
=
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
```

```
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: SSL
sequence: 20.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://198.154.68.90, Override trustpoint:
ASDM_TrustPoint12
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Destroying OCSP data handle 0xca2d27b8
Crypto CA thread sleeps!
CRYPTO_PKI: Attempting to find tunnel group for cert
with serial
number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
CRYPTO_PKI: Processing map rules for
DefaultCertificateMap.
CRYPTO_PKI: Processing map DefaultCertificateMap
sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED.
Peer cert field:
=
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map:
DefaultCertificateMap
sequence: 10.
CRYPTO_PKI: Ignoring match on map DefaultCertificateMap,
index 10 for
WebVPN group map processing. No tunnel group is
configured.
CRYPTO_PKI: Peer cert could not be authorized with map:
DefaultCertificateMap.
CRYPTO_PKI: Processing map rules for SSL.
CRYPTO_PKI: Processing map SSL sequence 20...
CRYPTO_PKI: Match of subject-name field to map PASSED.
Peer cert field:
=
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: SSL
sequence: 20.
CRYPTO_PKI: Ignoring match on map SSL, index 20 for
WebVPN group map
```

Figura C5: Saída de uma política de harmonização falhada do grupo do certificado

Figura C5: Saída de um certificado revogado

```
n %PI=X-3-7E17t02h7a Certinf icaHtue cnhta,in faioled
uvalidation=.
CMertifiIcLa,ted ccha=inl ais eibtrhaer tin,valdid cor
=noct
oamuthori,zed.
map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map:
DefaultCertificateMap
sequence: 10.
Tunnel Group Match on map DefaultCertificateMap sequence
# 10.
Group name is CAC-USERS
CRYPTO_PKI: Checking to see if an identical cert is
already in the database...
```

```
CRYPTO_PKI: looking for cert in handle=2467668, digest=
CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI: Cert not found in database.
CRYPTO_PKI: Looking for suitable trustpoints...
CRYPTO_PKI: Found a suitable authenticated trustpoint
trustpoint0.
CRYPTO_PKI: Certificate validation: Successful, status:
0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: Attempting to find OCSP override for peer
cert: serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
Hunt,ou=MIL,dc=ggsgseclab,dc=org, issuer_name:
cn=ggsgseclab,dc=ggsgseclab,dc=org.
CRYPTO_PKI: Processing map rules for
DefaultCertificateMap.
CRYPTO_PKI: Processing map DefaultCertificateMap
sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED.
Peer cert field:
= cn=Ethan Hunt,ou=MIL,dc=ggsgseclab,dc=org, map rule:
subject-name
ne "".
CRYPTO_PKI: Peer cert has been authorized by map:
DefaultCertificateMap
sequence: 10.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://ocsp.disa.mil, Override trustpoint: OCSP
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Found a subject match
ERROR: Certificate validation failed, Certificate is
revoked, serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
Hunt,ou=MIL,dc=ggsgseclab,dc=org
CRYPTO_PKI: Certificate not validated
```

Apêndice D – Verifique objetos LDAP no MS

No CD 2003 do servidor Microsoft, há as ferramentas adicionais que podem ser instaladas a fim ver a estrutura LDAP assim como os objetos LDAP/atributos. A fim instalar estas ferramentas, vá ao diretório do **apoio no** CD e então nas **ferramentas**. Instale **SUPTOOLS.MSI**.

Visor LDAP

- Após a instalação, escolha o **Iniciar > Executar**.
- Datilografe o **ldp**, a seguir clique a **aprovação**. Isto começa o visor LDAP.
- Escolha a **conexão > conectam**.
- Dê entrada com o nome do servidor e clique então a **aprovação**.
- Escolha a **conexão > o ligamento**.
- Incorpore um nome de usuário e senha.**Nota:** Você precisa direitos do administrador.
- Clique em **OK**.
- Objetos da vista LDAP. Veja a figura D1.**Figura D1: Visor LDAP**

Editor da relação dos serviços de diretório ativo

- No servidor ative directory, escolha o **Iniciar > Executar**.

- Datilografe **adsiedit.msc. Isto** começa o editor.
- Clicar com o botão direito em um objeto e clique **propriedades**.

Esta ferramenta mostra todos os atributos para objetos específicos. Veja a figura D2.

Figura D2: O ADSI edita

Apêndice E

Um perfil de AnyConnect pode ser criado e adicionado a uma estação de trabalho. O perfil pode prover vários valores tais como anfitriões ASA ou certificate parâmetros de harmonização tais como o nome destacado ou o expedidor. O perfil é armazenado como um arquivo do .xml e pode ser editado com bloco de notas. O arquivo pode ser adicionado a cada cliente manualmente ou ser empurrado do ASA com uma política do grupo. O arquivo é armazenado em:

```
C:\Documents and Settings\All Users\Application Data\Cisco\Cisco
AnyConnect VPN Client\Profile
```

Conclua estes passos:

1. Escolha o AnyConnectProfile.tmpl e abra o arquivo com bloco de notas.
2. Faça alterações apropriadas ao arquivo tal como o expedidor ou o IP de host. Veja a figura F1 por exemplo.
3. Quando terminado, salvar o arquivo como um .xml.

Esta é uma amostra de um arquivo do perfil XML do Cisco AnyConnect VPN Client.

Refira a documentação de Cisco AnyConnect com respeito ao Gerenciamento do perfil. Em curto:

- Um perfil deve excepcionalmente ser nomeado para sua empresa. Um exemplo é: CiscoProfile.xml
- O nome de perfil deve ser o mesmo mesmo se diferente para o grupo individual dentro da empresa.

Este arquivo é pretendido ser mantido por um administrador seguro do gateway e ser distribuído então com o software do cliente. O perfil baseado neste XML pode ser distribuído aos clientes a qualquer hora. Os mecanismos de distribuição apoiados são como um arquivo empacotado com a distribuição de software ou como parte do mecanismo automático da transferência. O mecanismo automático da transferência somente disponível com determinado Cisco fixa produtos de gateway.

Nota: Os administradores são incentivados fortemente validar o perfil que XML criam com o uso de uma ferramenta em linha da validação ou com a funcionalidade da importação do perfil no ASDM. A validação pode ser realizada com o AnyConnectProfile.xsd encontrado neste diretório. AnyConnectProfile é o elemento da raiz que representa o perfil do cliente de AnyConnect.

```
xml version="1.0" encoding="UTF-8" - -
<AnyConnectProfile
xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd"> !--- The ClientInitialization
section represents global settings !--- for the client.
In some cases, for example, BackupServerList, host
specific !--- overrides are possible. !-- --> -
<ClientInitialization> !--- The Start Before Logon
feature can be used to activate !--- the VPN as part of
```

```
the logon sequence. !--- UserControllable: Does the
administrator of this profile allow the user !--- to
control this attribute for their own use. Any user
setting !--- associated with this attribute is stored
elsewhere. --> <UseStartBeforeLogon
UserControllable="false">false</UseStartBeforeLogon> !--
- This control enables an administrator to have a one
time !--- message displayed prior to a users first
connection attempt. As an !--- example, the message can
be used to remind a user to insert their smart !--- card
into its reader. !--- The message to be used with this
control is localizable and can be !--- found in the
AnyConnect message catalog. !--- (default: "This is a
pre-connect reminder message.")
<ShowPreConnectMessage>false</ShowPreConnectMessage> !--
This section enables the definition of various
attributes !--- that can be used to refine client
certificate selection. --> - <CertificateMatch> !---
Certificate Distinguished Name matching allows for exact
!--- match criteria in the choosing of acceptable client
!--- certificates. - <DistinguishedName> -
<DistinguishedNameDefinition Operator="Equal"
Wildcard="Disabled"> <Name>ISSUER-CN</Name>
<Pattern>DoD-Issuer-ABC</Pattern>
</DistinguishedNameDefinition> </DistinguishedName>
</CertificateMatch> </ClientInitialization> - !-- This
section contains the list of hosts from which !--- the
user is able to select. - <ServerList> !--- This is the
data needed to attempt a connection to a specific !---
host. --> - <HostEntry> <HostName>host-02</HostName>
<HostAddress>host-02.dod.gov</HostAddress> </HostEntry>
- <HostEntry> <HostName>host-01</HostName>
<HostAddress>192.168.1.1</HostAddress> </HostEntry>
</ServerList> </AnyConnectProfile>
```

Informações Relacionadas

- Certificados & CRL especificados pelo X.509 e pelo RFC 3280
- OCSP especificado pelo RFC 2560
- Introdução da infraestrutura de chave pública
- “OCSP de pouco peso” perfilado pelo padrão de esboço
- SSL/TLS especificado pelo RFC 2246
- Suporte Técnico e Documentação - Cisco Systems