CS 3.x: Permissão e papéis estabelecidos do usuário

Índice

Introdução

Este documento descreve como estabelecer as permissões e os papéis aos usuários no Cisco Security Manager (CS).

Pré-requisitos

Requisitos

Este documento supõe que o CS está instalado e trabalha corretamente.

Componentes Utilizados

A informação neste documento é baseada no CS 3.1.

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.

Estabelecer permissões do usuário

O Cisco Security Manager autentica seu nome de usuário e senha antes que você possa entrar. Depois que são autenticados, o gerenciador de segurança estabelece seu papel dentro do aplicativo. Este papel define suas permissões (privilégios igualmente chamados), que são o grupo de tarefas ou as operações que você é autorizado para executar. Se você não é com certeza tarefas autorizadas ou dispositivos, os itens de menu relacionados, os artigos TOC, e os botões são hidden ou desabilitado. Além, uma mensagem diz-lhe que você não tem a permissão ver a informação selecionada ou executar a operação selecionada.

A authentication e autorização para o gerenciador de segurança é controlada pelo servidor ciscoworks ou pelo Serviço de controle de acesso Cisco Secure (ACS). À revelia, os CiscoWorks controlam a authentication e autorização, mas você pode mudar ao Cisco Secure ACS usando a página de instalação do modo AAA no CiscoWorks Common Services.

As vantagens principais de usar o Cisco Secure ACS são a capacidade para criar papéis de usuário altamente granulados com os grupos especializados das permissões (por exemplo, permitindo que o usuário configure determinada política datilografa mas não outro) e a capacidade para restringir usuários a determinados dispositivos configurando grupos de dispositivo de rede (NDGs).

Os seguintes assuntos descrevem permissões do usuário:

- Permissões do gerenciador de segurança
- Compreendendo papéis dos CiscoWorks
- Compreendendo papéis do Cisco Secure ACS
- Associações do padrão entre permissões e papéis no gerenciador de segurança

Permissões do gerenciador de segurança

O gerenciador de segurança classifica permissões nas categorias como mostrado:

1. **Vista** — Permite que você ver as configurações atual. Para mais informação, veja permissões da vista.
2. **Altere** — Permite que você mude as configurações atual. Para mais informação, veja para alterar permissões.
3. **Atribua** — Permite que você atribua políticas aos dispositivos e às topologias VPN. Para mais informação, veja para atribuir permissões
4. **Aprove** — Permite que você aprove alterações de política e trabalhos do desenvolvimento. Para mais informação, veja para aprovar permissões.

5. **Importação** — Permite que você importe as configurações que são distribuídas já em dispositivos no gerenciador de segurança.
6. **Distribua** — Permite que você distribua alterações de configuração aos dispositivos em sua rede e execute o rollback para retornar a uma configuração previamente distribuída.
7. **Controle** — Permite que você emita comandos aos dispositivos, tais como o sibilo.
8. **Submeta** — Permite que você submeta suas alterações de configuração para a aprovação.

- Quando você seleciona altere, atribua, aprove, importe, controle ou distribua permissões, você deve igualmente selecionar as permissões correspondentes da vista; se não, o gerenciador de segurança não funcionará corretamente.
- Quando você seleciona altere permissões da política, você deve igualmente selecionar a correspondência atribui e vê permissões da política.
- Quando você permite uma política que use objetos da política como parte de sua definição, você deve igualmente conceder permissões da vista a estes tipos de objeto. Por exemplo, se você seleciona a permissão para políticas de roteamento de alteração, você deve igualmente selecionar as permissões para objetos de rede e os papéis de vista da relação, que são os tipos de objeto exigidos por políticas de roteamento.
- O mesmo guarda verdadeiro ao permitir um objeto que use outros objetos como parte de sua definição. Por exemplo, se você seleciona a permissão para grupos de usuário de alteração, você deve igualmente selecionar as permissões para objetos de rede de visão, objetos ACL, e Grupos de servidores AAA.

Permissões da vista

As permissões (de leitura apenas) da vista no gerenciador de segurança são divididas nas categorias como mostrado:

- Permissões das políticas da vista
- Permissões dos objetos de vista
- Permissões adicionais da vista

Permissões das políticas da vista

O gerenciador de segurança inclui as seguintes permissões da vista para políticas:

1. **Vista > políticas > Firewall.** Permite que você ver as políticas de serviço de firewall (situadas no seletor de política sob o Firewall) em dispositivos PIX/ASA/FWSM, em dispositivos dos IOS Router, e do catalizador 6500/7600. Os exemplos de políticas de serviço de firewall incluem regras do acesso, regras AAA, e regras da inspeção.
2. **Vista > políticas > sistema da prevenção de intrusão.** Permite que você ver as políticas IPS (situadas no seletor de política sob o IPS), incluindo políticas para o IPS que é executado em IOS Router.
3. **Vista > políticas > imagem.** Permite você selecione um pacote da atualização de assinatura no assistente das atualizações IPS da aplicação (situado sob ferramentas > aplique a atualização IPS), mas não permite que você atribua o pacote aos dispositivos específicos, a menos que você igualmente tiver a permissão da alteração > das políticas > da imagem.
4. **Vista > políticas > NAT**. Permite que você ver políticas de tradução de endereço de rede em dispositivos e em IOS Router PIX/ASA/FWSM. Os exemplos das políticas de NAT incluem

regras estáticas e regras dinâmicas.

5. **Vista > políticas > VPN de Site-para-Site**. Permite que você ver políticas do VPN de Site-para-Site em dispositivos PIX/ASA/FWSM, em dispositivos dos IOS Router, e do catalizador 6500/7600. Os exemplos de políticas do VPN de Site-para-Site incluem propostas das propostas IKE, do IPsec, e chaves preshared.
6. **Vista > políticas > acesso remoto VPN**. Permite que você ver políticas do acesso remoto VPN em dispositivos PIX/ASA/FWSM, em dispositivos dos IOS Router, e do catalizador 6500/7600. Os exemplos de políticas do acesso remoto VPN incluem propostas das propostas IKE, do IPsec, e políticas PKI.
7. **Vista > políticas > SSL VPN**. Permite que você ver políticas de VPN SSL em dispositivos e em IOS Router PIX/ASA/FWSM, tais como o wizard VPN SSL.
8. **Vista > políticas > relações**. Permite que você ver as políticas da relação (situadas no seletor de política sob relações) em dispositivos PIX/ASA/FWSM, em IOS Router, em sensores IPS, e em dispositivos do catalizador 6500/7600.Em dispositivos PIX/ASA/FWSM, esta permissão cobre portas de hardware e ajustes da relação.Em IOS Router, esta permissão cobre ajustes básicos e avançados da relação, assim como outras políticas relação-relacionadas, tais como o DSL, o PVC, o PPP, e as políticas do discador.Em sensores IPS, esta permissão cobre interfaces física e mapas do sumário.Em dispositivos do catalizador 6500/7600, esta permissão cobre relações e configurações de vlan.
9. **Vista > políticas > construindo uma ponte sobre**. Permite que você ver as políticas da tabela ARP (situadas no seletor de política sob a plataforma > construindo uma ponte sobre) em dispositivos PIX/ASA/FWSM.
10. **Vista > políticas > administração do dispositivo**. Permite que você ver as políticas da administração do dispositivo (situadas no seletor de política sob a plataforma > o dispositivo Admin) em dispositivos PIX/ASA/FWSM, em dispositivos dos IOS Router, e do catalizador 6500/7600:Em dispositivos PIX/ASA/FWSM, os exemplos incluem o acesso de dispositivo policiam, políticas do acesso de servidor, e políticas do Failover.Em IOS Router, os exemplos incluem o acesso de dispositivo (que inclui a linha acesso) policiam, políticas do acesso de servidor, AAA, e fixam o abastecimento do dispositivo.Em sensores IPS, esta permissão cobre políticas do acesso de dispositivo e políticas do acesso de servidor.Em dispositivos do catalizador 6500/7600, esta permissão cobre ajustes IDSM e lista de acesso de vlan.
11. **Vista > políticas > identidade**. Permite que você ver as políticas da identidade (situadas no seletor de política sob a plataforma > a identidade) no Roteadores do Cisco IOS, incluindo o 802.1x e as políticas do Network Admission Control (NAC).
12. **Vista > políticas > registrando**. Permite que você ver as políticas de registro (situadas no seletor de política sob a plataforma > registrando) em dispositivos PIX/ASA/FWSM, em IOS Router, e em sensores IPS. Os exemplos de registrar políticas incluem a instalação, a instalação do server, e políticas de registro do servidor de SYSLOG.
13. **Vista > políticas > Multicast**. Permite que você ver as políticas do Multicast (situadas no seletor de política sob a plataforma > o Multicast) em dispositivos PIX/ASA/FWSM. Os exemplos de políticas do Multicast incluem o roteamento de transmissão múltipla e as políticas IGMP.
14. **Vista > políticas > QoS**. Permite que você ver as políticas de QoS (situadas no seletor de política sob a plataforma > o Qualidade de Serviço) no Roteadores do Cisco IOS.
15. **Vista > políticas > roteamento**. Permite que você ver as políticas de roteamento (situadas no seletor de política sob a plataforma > o roteamento) em dispositivos e em IOS Router PIX/ASA/FWSM. Os exemplos das políticas de roteamento incluem o OSPF, o RASGO, e

as políticas do roteamento estático.

16. **> segurança da vista > das políticas**. Permite que você ver as políticas de segurança (situadas no seletor de política sob o > segurança da plataforma) em dispositivos PIX/ASA/FWSM e em sensores IPS:Em dispositivos PIX/ASA/FWSM, as políticas de segurança incluem anti-falsificação, o fragmento, e as configurações de timeout.Em sensores IPS, as políticas de segurança incluem a obstrução de ajustes.
17. **Vista > políticas > regras da política de serviços**. Permite que você ver as políticas da regra da política de serviços (situadas no seletor de política sob regras da plataforma > da política de serviços) em dispositivos PIX 7.x/ASA. Os exemplos incluem filas de prioridade e IPS, QoS, e regras da conexão.
18. **Vista > políticas > preferências de usuário**. Permite que você ver a política do desenvolvimento (situada no seletor de política sob a plataforma > as preferências de usuário) em dispositivos PIX/ASA/FWSM. Esta política contém uma opção para cancelar todas as traduções NAT no desenvolvimento.
19. **Vista > políticas > dispositivo virtual**. Permite que você ver políticas virtuais do sensor em dispositivos IPS. Esta política é usada para criar sensores virtuais.
20. **Vista > políticas > FlexConfig**. Permite que você ver FlexConfigs, que são os comandos CLI e as instruções adicionais que podem ser distribuídos aos dispositivos PIX/ASA/FWSM, aos dispositivos dos IOS Router, e do catalizador 6500/7600.

Permissões dos objetos de vista

O gerenciador de segurança inclui as seguintes permissões da vista para objetos:

1. **A vista > objeta > Grupos de servidores AAA**. Permite que você ver objetos do Grupo de servidores AAA. Estes objetos são usados nas políticas que exigem serviços AAA (autenticação, autorização e relatório).
2. **A vista > objeta > servidores AAA**. Permite que você ver objetos do servidor AAA. Estes objetos representam os servidores AAA individuais que são definidos como parte de um Grupo de servidores AAA.
3. **A vista > objeta > listas de controle de acesso - Padrão/estendeu**. Permite que você ver o padrão e o ACL extendido objeta. Os objetos do ACL extendido são usados para uma variedade de políticas, tais como o NAT e o NAC, e estabelecendo o acesso VPN. Os objetos padrão ACL são usados para políticas como o OSPF e o SNMP, assim como estabelecendo o acesso VPN.
4. **A vista > objeta > listas de controle de acesso** - Web. Permite que você ver objetos da Web ACL. Os objetos da Web ACL são usados para executar o filtragem de conteúdo em políticas de VPN SSL.
5. **A vista > objeta > grupos de usuário ASA**. Permite que você ver objetos do grupo de usuário ASA. Estes objetos são configurados em ferramentas de segurança ASA no VPN, no acesso remoto VPN, e em configurações de VPN fáceis SSL.
6. **A vista > objeta > categorias**. Permite que você ver objetos da categoria. Estes objetos ajudam-no facilmente a identificar regras e objetos em tabelas das regras com o uso da cor.
7. **A vista > objeta > credenciais**. Permite que você ver objetos credenciais. Estes objetos são usados na configuração de VPN fácil durante o IKE Extended Authentication (Xauth).
8. **A vista > objeta > FlexConfigs**. Permite que você ver objetos de FlexConfig. Estes objetos, que contêm comandos configuration com instruções adicionais do linguagem de script, podem ser usados aos comandos configure que não são apoiados pela interface do

utilizador do gerenciador de segurança.

9. **A vista > objeta > propostas IKE**. Permite que você ver objetos da proposta IKE. Estes objetos contêm os parâmetros exigidos para propostas IKE em políticas do acesso remoto VPN.
10. **A vista > os objetos > inspecionam - Mapas da classe** - DNS. Permite que você ver objetos do mapa da classe DNS. Estes objetos combinam o tráfego DNS com os critérios específicos de modo que as ações possam ser executadas nesse tráfego.
11. **A vista > os objetos > inspecionam - Mapas da classe - FTP**. Permite que você ver objetos do mapa da classe FTP. Estes objetos combinam o tráfego FTP com os critérios específicos de modo que as ações possam ser executadas nesse tráfego.
12. **A vista > os objetos > inspecionam - Mapas da classe - HTTP**. Permite que você ver objetos do mapa da classe HTTP. Estes objetos combinam o tráfego de HTTP com os critérios específicos de modo que as ações possam ser executadas nesse tráfego.
13. **A vista > os objetos > inspecionam - Mapas da classe - IM**. Permite que você ver objetos do mapa da classe IM. Tráfego do fósforo IM destes objetos com critérios específicos de modo que as ações possam ser executadas nesse tráfego.
14. **A vista > os objetos > inspecionam - Mapas da classe - SORVO**. Permite que você ver objetos do mapa da classe do SORVO. Estes objetos combinam o tráfego do SORVO com os critérios específicos de modo que as ações possam ser executadas nesse tráfego.
15. **A vista > os objetos > inspecionam - Mapas da política - DNS.** Permite que você ver objetos do mapa de política DNS. Estes objetos são usados para criar mapas da inspeção para o tráfego DNS.
16. **A vista > os objetos > inspecionam - Mapas da política - FTP.** Permite que você ver objetos do mapa de política FTP. Estes objetos são usados para criar mapas da inspeção para o tráfego FTP.
17. **A vista > os objetos > inspecionam - Mapas da política - GTP**. Permite que você ver objetos do mapa de política GTP. Estes objetos são usados para criar mapas da inspeção para o tráfego GTP.
18. **A vista > os objetos > inspecionam - Mapas da política - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Permite que você ver os objetos do mapa da política HTTP criados para dispositivos e IOS Router ASA/PIX 7.1.x. Estes objetos são usados para criar mapas da inspeção para o tráfego de HTTP.
19. **A vista > os objetos > inspecionam - Mapas da política - HTTP (ASA7.2/PIX7.2)**. Permite que você ver os objetos do mapa da política HTTP criados para dispositivos ASA 7.2/PIX 7.2. Estes objetos são usados para criar mapas da inspeção para o tráfego de HTTP.
20. **A vista > os objetos > inspecionam - Mapas da política - IM (ASA7.2/PIX7.2)**. Permite que você ver os objetos do mapa de política IM criados para dispositivos ASA 7.2/PIX 7.2. Estes objetos são usados para criar mapas da inspeção para IM o tráfego.
21. **A vista > os objetos > inspecionam - Mapas da política - IM (IO)**. Permite que você ver os objetos do mapa de política IM criados para dispositivos de IOS. Estes objetos são usados para criar mapas da inspeção para IM o tráfego.
22. **A vista > os objetos > inspecionam - Mapas da política - SORVO**. Permite que você ver objetos do mapa de política do SORVO. Estes objetos são usados para criar mapas da inspeção para o tráfego do SORVO.
23. **A vista > os objetos > inspecionam - Expressões regulares**. Permite que você ver objetos da expressão regular. Estes objetos representam as expressões regulares individuais que são definidas como parte de um grupo da expressão regular.
24. **A vista > os objetos > inspecionam - Grupos das expressões regulares**. Permite que você

ver objetos do grupo da expressão regular. Estes objetos são usados por determinados mapas da classe e inspecionam mapas para combinar o texto dentro de um pacote.

25. **A vista > os objetos > inspecionam - O TCP traça**. Permite que você ver objetos do mapa TCP. Estes objetos personalizam a inspeção no fluxo de TCP nos ambos sentidos.
26. **A vista > objeta > papéis da relação**. Permite que você ver objetos do papel da relação. Estes objetos definem os testes padrões de nomeação que podem representar interfaces múltiplas em tipos diferentes de dispositivos. Os papéis da relação permitem-no de aplicar políticas às relações específicas em dispositivos múltiplos sem ter que manualmente definir o nome de cada relação.
27. **A vista > objeta > IPsec transforma grupos**. Permite que você ver o IPsec transformam objetos ajustados. Estes objetos compreendem uma combinação dos protocolos de segurança, dos algoritmos e dos outros ajustes que especificam exatamente como os dados no túnel de IPsec serão cifrados e autenticados.
28. **A vista > objeta > mapas do atributo LDAP**. Permite que você ver objetos do mapa do atributo LDAP. Estes objetos são usados para traçar nomes (definidos pelo utilizador) feitos sob encomenda do atributo aos nomes do atributo de Cisco LDAP.
29. **A vista > objeta > redes/anfitriões**. Permite que você ver objetos da rede/host. Estes objetos são coleções lógica dos endereços IP de Um ou Mais Servidores Cisco ICM NT que representam redes, anfitriões, ou ambos. Os objetos da rede/host permitem-no de definir políticas sem especificar cada rede ou de hospedá-las individualmente.
30. **A vista > objeta > registros PKI**. Permite que você ver objetos do registro PKI. Estes objetos definem os server do Certification Authority (CA) que se operam dentro de uma infraestrutura de chave pública.
31. **A vista > objeta > lista da transmissão da porta**. Permite que você ver objetos da lista da transmissão da porta. Estes objetos definem os mapeamentos dos números de porta em um cliente remoto ao endereço IP de Um ou Mais Servidores Cisco ICM NT do aplicativo e na porta atrás de um gateway de VPN SSL.
32. **A vista > objeta > configurações do Secure Desktop**. Permite que você ver objetos da configuração do Secure Desktop. Estes objetos são os componentes reusáveis, Nomeados que podem ser providos por políticas de VPN SSL para fornecer meios seguros de eliminar todos os traços de dados sensíveis que são compartilhados para a duração de uma sessão de VPN SSL.
33. **> serviços da vista > dos objetos - Listas de porta**. Permite que você ver objetos da lista de porta. Estes objetos, que contêm uns ou vários números de faixas de porta, são usados para aerodinamizar o processo de criar objetos do serviço.
34. **A vista > o > serviços/grupos de serviço dos objetos** permitem que você ver objetos do serviço e do grupo de serviço. Estes objetos são os mapeamentos definidos do protocolo e das definições de porta que descrevem os serviços de rede usados por políticas, tais como o Kerberos, SSH, e POP3.
35. **A vista > objeta > único sinal em server**. Permite que você ver o único sinal em objetos do server. Escolha Sinal-em (SSO) deixa usuários SSL VPN incorporar uma vez um nome de usuário e senha e poder alcançar serviços protegidos múltiplo e servidores de Web.
36. **A vista > objeta > monitores SLA**. Permite que você ver objetos do monitor SLA. Estes objetos são usados pelas ferramentas de segurança PIX/ASA que executam a versão 7.2 ou mais recente para executar o seguimento da rota. Esta característica fornece um método para seguir a Disponibilidade de uma rota principal e para instalar uma rota de backup se a rota principal falha.
37. **A vista > objeta > personalizações SSL VPN**. Permite que você ver objetos da

personalização SSL VPN. Estes objetos definem como mudar a aparência das páginas SSL VPN que são indicadas aos usuários, tais como o início de uma sessão/saída e os Home Page.

38. **A vista > objeta > gateways de VPN SSL**. Permite que você ver objetos do gateway de VPN SSL. Estes objetos definem os parâmetros que permitem o gateway de ser usados como um proxy para conexões aos recursos protegidos em seu SSL VPN.
39. **A vista > objeta > objetos do estilo**. Permite que você ver objetos do estilo. Estes objetos deixam-no configurar elementos do estilo, tais como características da fonte e cores, para personalizar a aparência da página SSL VPN que se publica aos usuários SSL VPN quando conectam à ferramenta de segurança.
40. **A vista > objeta > objetos do texto**. Permite que você ver objetos de forma livre do texto. Estes objetos compreendem um par do nome e do valor, onde o valor possa ser uma única corda, uma lista de cordas, ou uma tabela das cordas.
41. **A vista > objeta > intervalos de tempo.** Permite que você ver objetos do intervalo de tempo. Estes objetos são usados ao criar ACL com base no período e regras da inspeção. São usados igualmente ao definir grupos de usuário ASA para restringir o VPN alcançam às horas específicas durante a semana.
42. **A vista > objeta > fluxos de tráfego**. Permite que você ver objetos do fluxo de tráfego. Estes objetos definem fluxos de tráfego específicos para o uso dos dispositivos PIX 7.x/ASA 7.x.
43. **A vista > objeta > listas URL**. Permite que você ver objetos da lista URL. Estes objetos definem as URL que são indicadas na página portal após um login bem-sucedido. Isto permite usuários de alcançar os recursos disponíveis em Web site SSL VPN ao operar-se no modo de acesso dos sem clientes.
44. **A vista > objeta > grupos de usuário**. Permite que você ver objetos do grupo de usuário. Estes objetos definem grupos de clientes remotos que são usados em topologias fáceis, em acessos remoto VPN, e em SSL VPN VPN.
45. **Vista > objetos > listas de servidor das VITÓRIAS**. Permite que você ver objetos da lista de servidor das VITÓRIAS. Estes objetos representam os server das VITÓRIAS, que são usados por SSL VPN para alcançar ou compartilhar de arquivos em sistemas remotos.
46. **A vista > objeta > regras do DN interno**. Permite que você ver as regras DN usadas por políticas DN. Este é um objeto interno usado pelo gerenciador de segurança que não aparece no gerente do objeto da política.
47. **A vista > objeta > atualizações do cliente interno**. Este é um objeto interno exigido por objetos do grupo de usuário que não apareça no gerente do objeto da política.
48. **A vista > objeta > interno - Padrão ACE**. Este é um objeto interno para as entradas de controle de acesso padrão, que são usadas por objetos ACL.
49. **A vista > objeta > interno - ACE prolongados.** Este é um objeto interno para as entradas de controle de acesso prolongadas, que são usadas por objetos ACL.

Permissões adicionais da vista

O gerenciador de segurança inclui as seguintes permissões adicionais da vista:

1. **Vista > Admin**. Permite que você ver ajustes administrativos do gerenciador de segurança.
2. **Vista > CLI**. Permite que você ver os comandos CLI configurados em um dispositivo e inspecione os comandos que estão a ponto de ser distribuída.
3. **Vista > arquivo de configuração**. Permite que você ver a lista de configurações contidas no arquivo de configuração. Você não pode ver a configuração de dispositivo ou nenhuns

comandos CLI.
4. **Vista > dispositivos**. Permite que você ver dispositivos em vista do dispositivo e em toda a informação relacionada, incluindo seus ajustes do dispositivo, propriedades, atribuições, e assim por diante.
5. **Vista > gerenciadores de dispositivo**. Permite que você lance versões de leitura apenas dos gerenciadores de dispositivo para dispositivos individuais, tais como Roteador Cisco e Security Device Manager (SDM) para o Roteadores do Cisco IOS.
6. **Vista > topologia**. Permite que você ver os mapas configurados na opinião do mapa.

Altere permissões

Altere permissões (de leitura/gravação) no gerenciador de segurança são divididos nas categorias como mostrado:

- Altere permissões das políticas
- Altere permissões dos objetos
- Adicional altere permissões

Altere permissões das políticas

Nota: Quando você especifica altere permissões da política, certificam-se de que você selecionou a correspondência atribui e veem-se permissões da política também.

O gerenciador de segurança inclui o seguinte altera permissões para políticas:

1. **Altere > políticas > Firewall**. Permite que você altere as políticas de serviço de firewall (situadas no seletor de política sob o Firewall) em dispositivos PIX/ASA/FWSM, em dispositivos dos IOS Router, e do catalizador 6500/7600. Os exemplos de políticas de serviço de firewall incluem regras do acesso, regras AAA, e regras da inspeção.
2. **Altere > políticas > sistema da prevenção de intrusão**. Permite que você altere as políticas IPS (situadas no seletor de política sob o IPS), incluindo políticas para o IPS que é executado em IOS Router. Esta permissão igualmente permite que você ajuste assinaturas no assistente da atualização de assinatura (situado sob ferramentas > aplique a atualização IPS).
3. **Altere > políticas > imagem**. Permite que você atribua um pacote da atualização de assinatura aos dispositivos no assistente das atualizações IPS da aplicação (situado sob ferramentas > aplique a atualização IPS). Esta permissão igualmente permite que você atribua auto ajustes da atualização aos dispositivos específicos (situados sob a administração do gerenciador do ferramentas > segurança > atualizações IPS).
4. **Altere > políticas > NAT**. Permite que você altere políticas de tradução de endereço de rede em dispositivos e em IOS Router PIX/ASA/FWSM. Os exemplos das políticas de NAT incluem regras estáticas e regras dinâmicas.
5. **Altere > políticas > VPN de Site-para-Site**. Permite que você altere políticas do VPN de Site-para-Site em dispositivos PIX/ASA/FWSM, em dispositivos dos IOS Router, e do catalizador 6500/7600. Os exemplos de políticas do VPN de Site-para-Site incluem propostas das propostas IKE, do IPsec, e chaves preshared.
6. **Altere > políticas > acesso remoto VPN**. Permite que você altere políticas do acesso remoto VPN em dispositivos PIX/ASA/FWSM, em dispositivos dos IOS Router, e do catalizador

6500/7600. Os exemplos de políticas do acesso remoto VPN incluem propostas das propostas IKE, do IPsec, e políticas PKI.

7. **Altere > políticas > SSL VPN**. Permite que você altere políticas de VPN SSL em dispositivos e em IOS Router PIX/ASA/FWSM, tais como o wizard VPN SSL.
8. **Altere > políticas > relações**. Permite que você altere as políticas da relação (situadas no seletor de política sob relações) em dispositivos PIX/ASA/FWSM, em IOS Router, em sensores IPS, e em dispositivos do catalizador 6500/7600:Em dispositivos PIX/ASA/FWSM, esta permissão cobre portas de hardware e ajustes da relação.Em IOS Router, esta permissão cobre ajustes básicos e avançados da relação, assim como outras políticas relação-relacionadas, tais como o DSL, o PVC, o PPP, e as políticas do discador.Em sensores IPS, esta permissão cobre interfaces física e mapas do sumário.Em dispositivos do catalizador 6500/7600, esta permissão cobre relações e configurações de vlan.
9. **Altere > políticas > construindo uma ponte sobre**. Permite que você altere as políticas da tabela ARP (situadas no seletor de política sob a plataforma > construindo uma ponte sobre) em dispositivos PIX/ASA/FWSM.
10. **Altere > políticas > administração do dispositivo**. Permite que você altere as políticas da administração do dispositivo (situadas no seletor de política sob a plataforma > o dispositivo Admin) em dispositivos PIX/ASA/FWSM, em dispositivos dos IOS Router, e do catalizador 6500/7600:Em dispositivos PIX/ASA/FWSM, os exemplos incluem o acesso de dispositivo policiam, políticas do acesso de servidor, e políticas do Failover.Em IOS Router, os exemplos incluem o acesso de dispositivo (que inclui a linha acesso) policiam, políticas do acesso de servidor, AAA, e fixam o abastecimento do dispositivo.Em sensores IPS, esta permissão cobre políticas do acesso de dispositivo e políticas do acesso de servidor.Em dispositivos do catalizador 6500/7600, esta permissão cobre ajustes IDSM e lista de acesso de vlan.
11. **Altere > políticas > identidade**. Permite que você altere as políticas da identidade (situadas no seletor de política sob a plataforma > a identidade) no Roteadores do Cisco IOS, incluindo o 802.1x e as políticas do Network Admission Control (NAC).
12. **Altere > políticas > registrando**. Permite que você altere as políticas de registro (situadas no seletor de política sob a plataforma > registrando) em dispositivos PIX/ASA/FWSM, em IOS Router, e em sensores IPS. Os exemplos de registrar políticas incluem a instalação, a instalação do server, e políticas de registro do servidor de SYSLOG.
13. **Altere > políticas > Multicast**. Permite que você altere as políticas do Multicast (situadas no seletor de política sob a plataforma > o Multicast) em dispositivos PIX/ASA/FWSM. Os exemplos de políticas do Multicast incluem o roteamento de transmissão múltipla e as políticas IGMP.
14. **Altere > políticas > QoS**. Permite que você altere as políticas de QoS (situadas no seletor de política sob a plataforma > o Qualidade de Serviço) no Roteadores do Cisco IOS.
15. **Altere > políticas > roteamento**. Permite que você altere as políticas de roteamento (situadas no seletor de política sob a plataforma > o roteamento) em dispositivos e em IOS Router PIX/ASA/FWSM. Os exemplos das políticas de roteamento incluem o OSPF, o RASGO, e as políticas do roteamento estático.
16. **Altere > > segurança das políticas**. Permite que você altere as políticas de segurança (situadas no seletor de política sob o > segurança da plataforma) em dispositivos PIX/ASA/FWSM e em sensores IPS:Em dispositivos PIX/ASA/FWSM, as políticas de segurança incluem anti-falsificação, o fragmento, e as configurações de timeout.Em sensores IPS, as políticas de segurança incluem a obstrução de ajustes.
17. **Altere > políticas > regras da política de serviços**. Permite que você altere as políticas da

regra da política de serviços (situadas no seletor de política sob regras da plataforma > da política de serviços) em dispositivos PIX 7.x/ASA. Os exemplos incluem filas de prioridade e IPS, QoS, e regras da conexão.

18. **Altere > políticas > preferências de usuário**. Permite que você altere a política do desenvolvimento (situada no seletor de política sob a plataforma > as preferências de usuário) em dispositivos PIX/ASA/FWSM. Esta política contém uma opção para cancelar todas as traduções NAT no desenvolvimento.
19. **Altere > políticas > dispositivo virtual**. Permite que você altere políticas virtuais do sensor em dispositivos IPS. Use esta política para criar sensores virtuais.
20. **Altere > políticas > FlexConfig**. Permite que você altere FlexConfigs, que são os comandos CLI e as instruções adicionais que podem ser distribuídos aos dispositivos PIX/ASA/FWSM, aos dispositivos dos IOS Router, e do catalizador 6500/7600.

Altere permissões dos objetos

O gerenciador de segurança inclui as seguintes permissões da vista para objetos:

1. **Altere > objete > Grupos de servidores AAA**. Permite que você ver objetos do Grupo de servidores AAA. Estes objetos são usados nas políticas que exigem serviços AAA (autenticação, autorização e relatório).
2. **Altere > objete > servidores AAA**. Permite que você ver objetos do servidor AAA. Estes objetos representam os servidores AAA individuais que são definidos como parte de um Grupo de servidores AAA.
3. **Altere > objete > listas de controle de acesso - Padrão/estendeu**. Permite que você ver o padrão e o ACL extendido objeta. Os objetos do ACL extendido são usados para uma variedade de políticas, tais como o NAT e o NAC, e estabelecendo o acesso VPN. Os objetos padrão ACL são usados para políticas como o OSPF e o SNMP, assim como estabelecendo o acesso VPN.
4. **Altere > objete > listas de controle de acesso - Web**. Permite que você ver objetos da Web ACL. Os objetos da Web ACL são usados para executar o filtragem de conteúdo em políticas de VPN SSL.
5. **Altere > objete >** grupos de usuário **ASA**. Permite que você ver objetos do grupo de usuário ASA. Estes objetos são configurados em ferramentas de segurança ASA no VPN, no acesso remoto VPN, e em configurações de VPN fáceis SSL.
6. **Altere > objete > categorias**. Permite que você ver objetos da categoria. Estes objetos ajudam-no facilmente a identificar regras e objetos em tabelas das regras com o uso da cor.
7. **Altere > objete > credenciais**. Permite que você ver objetos credenciais. Estes objetos são usados na configuração de VPN fácil durante o IKE Extended Authentication (Xauth).
8. **Altere > objete > FlexConfigs**. Permite que você ver objetos de FlexConfig. Estes objetos, que contêm comandos configuration com instruções adicionais do linguagem de script, podem ser usados aos comandos configure que não são apoiados pela interface do utilizador do gerenciador de segurança.
9. **Altere > objete > propostas IKE**. Permite que você ver objetos da proposta IKE. Estes objetos contêm os parâmetros exigidos para propostas IKE em políticas do acesso remoto VPN.
10. **Altere > objetos > inspecionam - Mapas da classe - DNS**. Permite que você ver objetos do mapa da classe DNS. Estes objetos combinam o tráfego DNS com os critérios específicos de modo que as ações possam ser executadas nesse tráfego.

11. **Altere > objetos > inspecionam - Mapas da classe - FTP**. Permite que você ver objetos do mapa da classe FTP. Estes objetos combinam o tráfego FTP com os critérios específicos de modo que as ações possam ser executadas nesse tráfego.
12. **Altere > objetos > inspecionam - Mapas da classe - HTTP**. Permite que você ver objetos do mapa da classe HTTP. Estes objetos combinam o tráfego de HTTP com os critérios específicos de modo que as ações possam ser executadas nesse tráfego.
13. **Altere > objetos > inspecionam - Mapas da classe - IM**. Permite que você ver objetos do mapa da classe IM. Tráfego do fósforo IM destes objetos com critérios específicos de modo que as ações possam ser executadas nesse tráfego.
14. **Altere > objetos > inspecionam - Mapas da classe - SORVO**. Permite que você ver objetos do mapa da classe do SORVO. Estes objetos combinam o tráfego do SORVO com os critérios específicos de modo que as ações possam ser executadas nesse tráfego.
15. **Altere > objetos > inspecionam - Mapas da política - DNS**. Permite que você ver objetos do mapa de política DNS. Estes objetos são usados para criar mapas da inspeção para o tráfego DNS.
16. **Altere > objetos > inspecionam - Mapas da política - FTP**. Permite que você ver objetos do mapa de política FTP. Estes objetos são usados para criar mapas da inspeção para o tráfego FTP.
17. **Altere > objetos > inspecionam - Mapas da política - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Permite que você ver os objetos do mapa da política HTTP criados para dispositivos e IOS Router ASA/PIX 7.x. Estes objetos são usados para criar mapas da inspeção para o tráfego de HTTP.
18. **Altere > objetos > inspecionam - Mapas da política - HTTP (ASA7.2/PIX7.2)**. Permite que você ver os objetos do mapa da política HTTP criados para dispositivos ASA 7.2/PIX 7.2. Estes objetos são usados para criar mapas da inspeção para o tráfego de HTTP.
19. **Altere > objetos > inspecionam - Mapas da política - IM (ASA7.2/PIX7.2)**. Permite que você ver os objetos do mapa de política IM criados para dispositivos ASA 7.2/PIX 7.2. Estes objetos são usados para criar mapas da inspeção para IM o tráfego.
20. **Altere > objetos > inspecionam - Mapas da política - IM (IO)**. Permite que você ver os objetos do mapa de política IM criados para dispositivos de IOS. Estes objetos são usados para criar mapas da inspeção para IM o tráfego.
21. **Altere > objetos > inspecionam - Mapas da política - SORVO**. Permite que você ver objetos do mapa de política do SORVO. Estes objetos são usados para criar mapas da inspeção para o tráfego do SORVO.
22. **Altere > objetos > inspecionam - Expressões regulares**. Permite que você ver objetos da expressão regular. Estes objetos representam as expressões regulares individuais que são definidas como parte de um grupo da expressão regular.
23. **Altere > objetos > inspecionam - Grupos das expressões regulares**. Permite que você ver objetos do grupo da expressão regular. Estes objetos são usados por determinados mapas da classe e inspecionam mapas para combinar o texto dentro de um pacote.
24. **Altere > objetos > inspecionam - O TCP traça**. Permite que você ver objetos do mapa TCP. Estes objetos personalizam a inspeção no fluxo de TCP nos ambos sentidos.
25. **Altere > objete > papéis da relação**. Permite que você ver objetos do papel da relação. Estes objetos definem os testes padrões de nomeação que podem representar interfaces múltiplas em tipos diferentes de dispositivos. Os papéis da relação permitem-no de aplicar políticas às relações específicas em dispositivos múltiplos sem ter que manualmente definir o nome de cada relação.
26. **Altere > objete > IPsec transformam grupos**. Permite que você ver o IPsec transformam

objetos ajustados. Estes objetos compreendem uma combinação dos protocolos de segurança, dos algoritmos e dos outros ajustes que especificam exatamente como os dados no túnel de IPsec serão cifrados e autenticados.

27. **Altere > objete > mapas do atributo LDAP**. Permite que você ver objetos do mapa do atributo LDAP. Estes objetos são usados para traçar nomes (definidos pelo utilizador) feitos sob encomenda do atributo aos nomes do atributo de Cisco LDAP.
28. **Altere > objete > redes/anfitriões**. Permite que você ver objetos da rede/host. Estes objetos são coleções lógica dos endereços IP de Um ou Mais Servidores Cisco ICM NT que representam redes, anfitriões, ou ambos. Os objetos da rede/host permitem-no de definir políticas sem especificar cada rede ou de hospedá-las individualmente.
29. **Altere > objete > registros PKI**. Permite que você ver objetos do registro PKI. Estes objetos definem os server do Certification Authority (CA) que se operam dentro de uma infraestrutura de chave pública.
30. **Altere > objete > lista da transmissão da porta**. Permite que você ver objetos da lista da transmissão da porta. Estes objetos definem os mapeamentos dos números de porta em um cliente remoto ao endereço IP de Um ou Mais Servidores Cisco ICM NT do aplicativo e na porta atrás de um gateway de VPN SSL.
31. **Altere > objete > configurações do Secure Desktop**. Permite que você ver objetos da configuração do Secure Desktop. Estes objetos são os componentes reusáveis, Nomeados que podem ser providos por políticas de VPN SSL para fornecer meios seguros de eliminar todos os traços de dados sensíveis que são compartilhados para a duração de uma sessão de VPN SSL.
32. **Altere > > serviços dos objetos - Listas de porta**. Permite que você ver objetos da lista de porta. Estes objetos, que contêm uns ou vários números de faixas de porta, são usados para aerodinamizar o processo de criar objetos do serviço.
33. **Altere > > serviços/grupos de serviço dos objetos.** Permite que você ver o serviço e o grupo de serviço objeta. Estes objetos são os mapeamentos definidos do protocolo e das definições de porta que descrevem os serviços de rede usados por políticas, tais como o Kerberos, SSH, e POP3.
34. **Altere > objete > único sinal em server.** Permite que você ver o único sinal em objetos do server. Escolha Sinal-em (SSO) deixa usuários SSL VPN incorporar uma vez um nome de usuário e senha e poder alcançar serviços protegidos múltiplo e servidores de Web.
35. **Altere > objete > monitores SLA**. Permite que você ver objetos do monitor SLA. Estes objetos são usados pelas ferramentas de segurança PIX/ASA que executam a versão 7.2 ou mais recente para executar o seguimento da rota. Esta característica fornece um método para seguir a Disponibilidade de uma rota principal e para instalar uma rota de backup se a rota principal falha.
36. **Altere > objete > personalizações SSL VPN**. Permite que você ver objetos da personalização SSL VPN. Estes objetos definem como mudar a aparência das páginas SSL VPN que são indicadas aos usuários, tais como o início de uma sessão/saída e os Home Page.
37. **Altere > objete > gateways de VPN SSL**. Permite que você ver objetos do gateway de VPN SSL. Estes objetos definem os parâmetros que permitem o gateway de ser usados como um proxy para conexões aos recursos protegidos em seu SSL VPN.
38. **Altere > objete > objetos do estilo**. Permite que você ver objetos do estilo. Estes objetos deixam-no configurar elementos do estilo, tais como características da fonte e cores, para personalizar a aparência da página SSL VPN que se publica aos usuários SSL VPN quando conectam à ferramenta de segurança.

39. **Altere > objete > objetos do texto**. Permite que você ver objetos de forma livre do texto. Estes objetos compreendem um par do nome e do valor, onde o valor possa ser uma única corda, uma lista de cordas, ou uma tabela das cordas.
40. **Altere > objete > intervalos de tempo.** Permite que você ver objetos do intervalo de tempo. Estes objetos são usados ao criar ACL com base no período e regras da inspeção. São usados igualmente ao definir grupos de usuário ASA para restringir o VPN alcançam às horas específicas durante a semana.
41. **Altere > objete > fluxos de tráfego**. Permite que você ver objetos do fluxo de tráfego. Estes objetos definem fluxos de tráfego específicos para o uso dos dispositivos PIX 7.x/ASA 7.x.
42. **Altere > objete > listas URL**. Permite que você ver objetos da lista URL. Estes objetos definem as URL que são indicadas na página portal após um login bem-sucedido. Isto permite usuários de alcançar os recursos disponíveis em Web site SSL VPN ao operar-se no modo de acesso dos sem clientes.
43. **Altere > objete > grupos de usuário**. Permite que você ver objetos do grupo de usuário. Estes objetos definem grupos de clientes remotos que são usados em topologias fáceis, em acessos remoto VPN, e em SSL VPN VPN
44. **Altere > objetos > listas de servidor das VITÓRIAS**. Permite que você ver objetos da lista de servidor das VITÓRIAS. Estes objetos representam os server das VITÓRIAS, que são usados por SSL VPN para alcançar ou compartilhar de arquivos em sistemas remotos.
45. **Altere > objete > regras do DN interno.** Permite que você ver as regras DN usadas por políticas DN. Este é um objeto interno usado pelo gerenciador de segurança que não aparece no gerente do objeto da política.
46. **Altere > objete > atualizações do cliente interno**. Este é um objeto interno exigido por objetos do grupo de usuário que não apareça no gerente do objeto da política.
47. **Altere > objete > interno - Padrão ACE**. Este é um objeto interno para as entradas de controle de acesso padrão, que são usadas por objetos ACL.
48. **Altere > objete > interno - ACE prolongado**. Este é um objeto interno para as entradas de controle de acesso prolongadas, que são usadas por objetos ACL.

Adicional altere permissões

O gerenciador de segurança inclui o adicional altera permissões como mostrado:

1. **Altere > Admin**. Permite que você altere ajustes administrativos do gerenciador de segurança.
2. **Altere > arquivo de configuração**. Permite que você altere a configuração de dispositivo no arquivo de configuração. Além, permite que você adicione configurações ao arquivo e personalize a ferramenta do arquivo de configuração.
3. **Altere > dispositivos**. Permite que você adicione e suprima de dispositivos, assim como alteram propriedades e atributos do dispositivo. Para descobrir as políticas no dispositivo que está sendo adicionado, você deve igualmente permitir a permissão da importação. Além, se você permite a permissão da alteração > dos dispositivos, certifique-se de que você igualmente permite a permissão da atribuição > das políticas > das relações.
4. **Altere > hierarquia**. Permite que você altere grupos do dispositivo.
5. **Altere > topologia**. Permite que você altere mapas na opinião do mapa.

Atribua permissões

O gerenciador de segurança inclui as permissões da atribuição da política como mostrado:

1. **Atribua > políticas > Firewall**. Permite que você atribua as políticas de serviço de firewall (situadas no seletor de política sob o Firewall) aos dispositivos PIX/ASA/FWSM, aos dispositivos dos IOS Router, e do catalizador 6500/7600. Os exemplos de políticas de serviço de firewall incluem regras do acesso, regras AAA, e regras da inspeção.
2. **Atribua > políticas > sistema da prevenção de intrusão**. Permite que você atribua as políticas IPS (situadas no seletor de política sob o IPS), incluindo políticas para o IPS que é executado em IOS Router.
3. **Atribua > políticas > imagem**. Esta permissão não é usada atualmente pelo gerenciador de segurança.
4. **Atribua > políticas > NAT**. Permite que você atribua políticas de tradução de endereço de rede aos dispositivos e aos IOS Router PIX/ASA/FWSM. Os exemplos das políticas de NAT incluem regras estáticas e regras dinâmicas.
5. **Atribua > políticas > VPN de Site-para-Site**. Permite que você atribua políticas do VPN de Site-para-Site aos dispositivos PIX/ASA/FWSM, aos dispositivos dos IOS Router, e do catalizador 6500/7600. Os exemplos de políticas do VPN de Site-para-Site incluem propostas das propostas IKE, do IPsec, e chaves preshared.
6. **Atribua > políticas > acesso remoto VPN**. Permite que você atribua políticas do acesso remoto VPN aos dispositivos PIX/ASA/FWSM, aos dispositivos dos IOS Router, e do catalizador 6500/7600. Os exemplos de políticas do acesso remoto VPN incluem propostas das propostas IKE, do IPsec, e políticas PKI.
7. **Atribua > políticas > SSL VPN**. Permite que você atribua políticas de VPN SSL aos dispositivos e aos IOS Router PIX/ASA/FWSM, tais como o wizard VPN SSL.
8. **Atribua > políticas > relações**. Permite que você atribua as políticas da relação (situadas no seletor de política sob relações) aos dispositivos PIX/ASA/FWSM, aos dispositivos dos IOS Router, e do catalizador 6500/7600:Em dispositivos PIX/ASA/FWSM, esta permissão cobre portas de hardware e ajustes da relação.Em IOS Router, esta permissão cobre ajustes básicos e avançados da relação, assim como outras políticas relação-relacionadas, tais como o DSL, o PVC, o PPP, e as políticas do discador.Em dispositivos do catalizador 6500/7600, esta permissão cobre relações e configurações de vlan.
9. **Atribua > políticas > construindo uma ponte sobre**. Permite que você atribua as políticas da tabela ARP (situadas no seletor de política sob a plataforma > construindo uma ponte sobre) aos dispositivos PIX/ASA/FWSM.
10. **Atribua > políticas > administração do dispositivo**. Permite que você atribua as políticas da administração do dispositivo (situadas no seletor de política sob a plataforma > o dispositivo Admin) aos dispositivos PIX/ASA/FWSM, aos dispositivos dos IOS Router, e do catalizador 6500/7600:Em dispositivos PIX/ASA/FWSM, os exemplos incluem o acesso de dispositivo policiam, políticas do acesso de servidor, e políticas do Failover.Em IOS Router, os exemplos incluem o acesso de dispositivo (que inclui a linha acesso) policiam, políticas do acesso de servidor, AAA, e fixam o abastecimento do dispositivo.Em sensores IPS, esta permissão cobre políticas do acesso de dispositivo e políticas do acesso de servidor.Em dispositivos do catalizador 6500/7600, esta permissão cobre ajustes IDSM e lista de acesso de vlan.
11. **Atribua > políticas > identidade**. Permite que você atribua as políticas da identidade (situadas no seletor de política sob a plataforma > a identidade) ao Roteadores do Cisco IOS, incluindo o 802.1x e as políticas do Network Admission Control (NAC).
12. **Atribua > políticas > registrando**. Permite que você atribua as políticas de registro (situadas

no seletor de política sob a plataforma > registrando) aos dispositivos e aos IOS Router PIX/ASA/FWSM. Os exemplos de registrar políticas incluem a instalação, a instalação do server, e políticas de registro do servidor de SYSLOG.

13. **Atribua > políticas > Multicast**. Permite que você atribua as políticas do Multicast (situadas no seletor de política sob a plataforma > o Multicast) aos dispositivos PIX/ASA/FWSM. Os exemplos de políticas do Multicast incluem o roteamento de transmissão múltipla e as políticas IGMP.
14. **Atribua > políticas > QoS**. Permite que você atribua as políticas de QoS (situadas no seletor de política sob a plataforma > o Qualidade de Serviço) ao Roteadores do Cisco IOS.
15. **Atribua > políticas > roteamento**. Permite que você atribua as políticas de roteamento (situadas no seletor de política sob a plataforma > o roteamento) aos dispositivos e aos IOS Router PIX/ASA/FWSM. Os exemplos das políticas de roteamento incluem o OSPF, o RASGO, e as políticas do roteamento estático.
16. **Atribua > > segurança das políticas**. Permite que você atribua as políticas de segurança (situadas no seletor de política sob o > segurança da plataforma) aos dispositivos PIX/ASA/FWSM. As políticas de segurança incluem anti-falsificação, o fragmento, e as configurações de timeout.
17. **Atribua > políticas > regras da política de serviços**. Permite que você atribua as políticas da regra da política de serviços (situadas no seletor de política sob regras da plataforma > da política de serviços) aos dispositivos PIX 7.x/ASA. Os exemplos incluem filas de prioridade e IPS, QoS, e regras da conexão.
18. **Atribua > políticas > preferências de usuário**. Permite que você atribua a política do desenvolvimento (situada no seletor de política sob a plataforma > as preferências de usuário) aos dispositivos PIX/ASA/FWSM. Esta política contém uma opção para cancelar todas as traduções NAT no desenvolvimento.
19. **Atribua > políticas > dispositivo virtual**. Permite que você atribua políticas virtuais do sensor aos dispositivos IPS. Use esta política para criar sensores virtuais.
20. **Atribua > políticas > FlexConfig**. Permite que você atribua FlexConfigs, que são os comandos CLI e as instruções adicionais que podem ser distribuídos aos dispositivos PIX/ASA/FWSM, aos dispositivos dos IOS Router, e do catalizador 6500/7600.

Nota: Quando você especifica atribua permissões, certificam-se de que você selecionou as permissões correspondentes da vista também.

Aprove permissões

O gerenciador de segurança fornece as permissões da aprovação como mostrado:

1. **Aprove > CLI**. Permite que você aprove as mudanças do comando CLI contidas em um trabalho do desenvolvimento.
2. **Aprove > política**. Permite que você aprove as alterações de configuração contidas nas políticas que foram configuradas em uma atividade dos trabalhos.

Compreendendo papéis dos CiscoWorks

Quando os usuários são criados no CiscoWorks Common Services, eles estão atribuídos uns ou vários papéis. As permissões associadas com cada papel determinam as operações que cada

usuário é autorizado executar no gerenciador de segurança.

Os seguintes assuntos descrevem papéis dos CiscoWorks:

- Papéis do padrão do CiscoWorks Common Services
- Atribuindo papéis aos usuários no CiscoWorks Common Services

Papéis do padrão do CiscoWorks Common Services

O CiscoWorks Common Services contém os seguintes papéis do padrão:

1. **Help desk** — Os usuários do help desk podem ver (mas para não alterar) dispositivos, políticas, objetos, e mapas de topologia.
2. **Operador de rede** — Além do que permissões da vista, os operadores de rede podem ver ajustes administrativos dos comandos CLI e do gerenciador de segurança. Os operadores de rede podem igualmente alterar os comandos do arquivo de configuração e da edição (tais como o sibilo) aos dispositivos.
3. **Approver** — Além do que permissões da vista, os approvers podem aprovar ou rejeitar trabalhos do desenvolvimento. Não podem executar o desenvolvimento.
4. **Administrador de rede** — Os administradores de rede têm a vista completa e alteram permissões, à exceção de alterar ajustes administrativos. Podem descobrir dispositivos e as políticas configuradas nestes dispositivos, para atribuir políticas aos dispositivos, e comandos da edição aos dispositivos. Os administradores de rede não podem aprovar atividades ou trabalhos do desenvolvimento; contudo, podem distribuir os trabalhos que foram aprovados por outro.
5. **Administrador de sistema** — Os administradores de sistema têm o acesso completo a todas as permissões do gerenciador de segurança, incluindo a alteração, a atribuição da política, a atividade e a aprovação de trabalho, descoberta, desenvolvimento, e emitindo comandos aos dispositivos.

Nota: Os papéis adicionais, tais como dados da exportação, puderam ser indicados em serviços comuns se os aplicativos adicionais são instalados no server. O papel dos dados da exportação é para desenvolvedores de terceira parte e não é usado pelo gerenciador de segurança.

Dica: Embora você não possa mudar a definição de papéis dos CiscoWorks, você pode definir que papéis são atribuídos a cada usuário. Para mais informação, veja a atribuição de papéis aos usuários no CiscoWorks Common Services.

Atribuindo papéis aos usuários no CiscoWorks Common Services

O CiscoWorks Common Services permite-o de definir que papéis são atribuídos a cada usuário. Mudando a definição do papel para um usuário, você muda os tipos de operações que este usuário é autorizado executa no gerenciador de segurança. Por exemplo, se você atribui o papel do help desk, o usuário é limitado para ver operações e não pode alterar nenhuns dados. Contudo, se você atribui o papel do operador de rede, o usuário pode igualmente alterar o arquivo de configuração. Você pode atribuir papéis múltiplos a cada usuário.

Nota: Você deve reiniciar o gerenciador de segurança após ter feito mudanças às permissões do usuário.

Procedimento:

1. Em serviços comuns, o **> segurança** seleto do **server**, seleciona então o **Gerenciamento > o usuário local de confiança do servidor único Setup do** TOC.**Dica:** Para alcançar a página de instalação do usuário local de dentro do gerenciador de segurança, a administração do gerenciador seleta do ferramentas > segurança > a Segurança do server, clicam então a instalação do usuário local.
2. Selecione a caixa de verificação ao lado de um usuário existente, a seguir clique-a **editam**.
3. Na página da informação sobre o usuário, selecione os papéis para atribuir a este usuário clicando as caixas de seleção.Para obter mais informações sobre de cada papel, veja papéis do padrão do CiscoWorks Common Services.
4. Clique a **APROVAÇÃO** para salvar suas mudanças.
5. Reinicie o gerenciador de segurança.

Compreendendo papéis do Cisco Secure ACS

O Cisco Secure ACS fornece a maior flexibilidade para controlar permissões do gerenciador de segurança do que fazem os CiscoWorks porque apoia os papéis característicos da aplicação que você pode configurar. Cada papel é composto de um grupo de permissões que determinam o nível da autorização às tarefas do gerenciador de segurança. No Cisco Secure ACS, você atribui um papel a cada grupo de usuário (e opcionalmente, aos usuários individuais também), que permite cada usuário nesse grupo de executar as operações autorizou pelas permissões definidas para esse papel.

Além, você pode atribuir estes papéis aos grupos do dispositivo do Cisco Secure ACS, permitindo que as permissões sejam diferenciadas em conjuntos de dispositivo diferentes.

Nota: Os grupos do dispositivo do Cisco Secure ACS são independente de grupos do dispositivo do gerenciador de segurança.

Os seguintes assuntos descrevem papéis do Cisco Secure ACS:

- Papéis do padrão do Cisco Secure ACS
- Personalizando papéis do Cisco Secure ACS

Papéis do padrão do Cisco Secure ACS

O Cisco Secure ACS inclui os mesmos papéis que CiscoWorks (veja compreendendo papéis dos CiscoWorks), mais estes papéis adicionais:

1. **Segurança Approver** — Os approvers da Segurança podem ver (mas para não alterar) dispositivos, políticas, objetos, mapas, comandos CLI, e ajustes administrativos. Além, os approvers da Segurança podem aprovar ou rejeitar as alterações de configuração contidas em uma atividade. Não podem aprovar ou rejeitar o trabalho do desenvolvimento, nem podem executar o desenvolvimento.
2. **Administrador de segurança** — Além do que ter permissões da vista, os administradores de segurança podem alterar dispositivos, grupos do dispositivo, políticas, objetos, e mapas de topologia. Podem igualmente atribuir políticas aos dispositivos e às topologias VPN, e executam a descoberta para importar dispositivos novos no sistema.
3. **Administrador de rede** — Além do que permissões da vista, os administradores de rede podem alterar o arquivo de configuração, executar o desenvolvimento, e os comandos da

edição aos dispositivos.

Nota: As permissões contidas no papel de administrador de rede do Cisco Secure ACS são diferentes daquelas contidas no papel de administrador de rede dos CiscoWorks. Para mais informação, veja compreendendo papéis dos CiscoWorks.

Ao contrário dos CiscoWorks, o Cisco Secure ACS permite-o de personalizar as permissões associadas com cada papel do gerenciador de segurança. Para obter mais informações sobre de alterar os papéis do padrão, veja a personalização de papéis do Cisco Secure ACS.

Nota: O Cisco Secure ACS 3.3 ou mais atrasado deve ser instalado para a autorização do gerenciador de segurança.

Personalizando papéis do Cisco Secure ACS

O Cisco Secure ACS permite-o de alterar as permissões associadas com cada papel do gerenciador de segurança. Você pode igualmente personalizar o Cisco Secure ACS criando papéis de usuário especializados com as permissões que são visadas às tarefas particulares do gerenciador de segurança.

Nota: Você deve reiniciar o gerenciador de segurança após ter feito mudanças às permissões do usuário.

Procedimento:

1. No Cisco Secure ACS, clique **componentes de perfil compartilhado na** barra de navegação.
2. Clique o **Cisco Security Manager na** página compartilhada dos componentes. Os papéis que são configurados para o gerenciador de segurança são indicados.
3. Escolha fazer entre o seguinte:Para criar um papel, o clique **adiciona**. Vá para a etapa 4.Para alterar um papel existente, clique o papel. Vá para a Etapa 5.
4. Dê entrada com um nome para o papel e, opcionalmente, uma descrição.
5. Selecione e deselect as caixas de seleção na árvore das permissões para definir as permissões para este papelSelecionar a caixa de verificação para um ramo da árvore seleciona todas as permissões nesse ramo. Por exemplo, selecionar **atribui** seleciona todas as permissões da atribuição.Para uma lista completa de permissões do gerenciador de segurança, veja permissões do gerenciador de segurança.**Nota:** Quando você seleciona altere, aprove, atribua, importe, controle ou distribua permissões, você deve igualmente selecionar as permissões correspondentes da vista; se não, o gerenciador de segurança não funcionará corretamente.
6. O clique **submete-se** para salvar suas mudanças.
7. Gerenciador de segurança do reinício.

Associações do padrão entre permissões e papéis no gerenciador de segurança

Esta tabela mostra como as permissões do gerenciador de segurança são associadas com os papéis do CiscoWorks Common Services e os papéis do padrão no Cisco Secure ACS.

Permissões	Papéis							

	System Admin	Segurança Admin (ACS)	Segurança Aprover (ACS)	Rede Admin (CW)	Rede Admin (ACS)	Approver	Operador de rede	Helpdesk
Permissões da vista								
Dispositivo da vista	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Política da vista	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Objetos de vista	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Topologia da vista	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Vista CLI	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Não
Vista Admin	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Não
Arquivo de configuração da vista	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Gerenciadores de dispositivo da vista	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Não
Altere permissões								
Altere o dispositivo	Sim	Sim	Não	Sim	Não	Não	Não	Não
Altere a hierarquia	Sim	Sim	Não	Sim	Não	Não	Não	Não
Altere a política	Sim	Sim	Não	Sim	Não	Não	Não	Não
Altere a imagem	Sim	Sim	Não	Sim	Não	Não	Não	Não
Altere objetos	Sim	Sim	Não	Sim	Não	Não	Não	Não
Altere a topologia	Sim	Sim	Não	Sim	Não	Não	Não	Não
Altere o Admin	Sim	Não	Não	Não	Não	Não	Não	Não
Altere o arquivo de configuração	Sim	Sim	Não	Sim	Sim	Não	Sim	Não

o								
Permissões adicionais								
Atribua a política	Sim	Sim	Não	Sim	Não	Não	Não	Não
Aprove a política	Sim	Não	Sim	Não	Não	Não	Não	Não
Aprove o CLI	Sim	Não	Não	Não	Não	Sim	Não	Não
Descubra (importação)	Sim	Sim	Não	Sim	Não	Não	Não	Não
Distribua	Sim	Não	Não	Sim	Sim	Não	Não	Não
Controle	Sim	Não	Não	Sim	Sim	Não	Sim	Não
Submeta	Sim	Sim	Não	Sim	Não	Não	Não	Não

Informações Relacionadas

- Página de suporte do Cisco Security Manager
- Suporte Técnico e Documentação - Cisco Systems