CSM 3.x: Gebruikerstoegang en -rollen instellen

Inhoud

Inleiding

Dit document beschrijft hoe u de toegangsrechten en rollen aan de gebruikers in Cisco Security Manager (CSM) kunt instellen.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat de CSM is geïnstalleerd en correct werkt.

Gebruikte componenten

De informatie in dit document is gebaseerd op CSM 3.1.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van

elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Gebruikershandleidingen instellen

Cisco Security Manager authenticeert uw gebruikersnaam en wachtwoord voordat u kunt inloggen. Nadat ze echt zijn gemaakt, stelt Security Manager uw rol in de toepassing vast. Deze rol definieert uw rechten (ook wel rechten genoemd), die de reeks taken of bewerkingen zijn die u mag uitvoeren. Als u niet bent geautoriseerd voor bepaalde taken of apparaten, worden de bijbehorende menu-items, TOC-items en knoppen verborgen of uitgeschakeld. Daarnaast wordt in een bericht verteld dat u geen toestemming hebt om de geselecteerde informatie te bekijken of de geselecteerde handeling uit te voeren.

Verificatie en toestemming voor Security Manager wordt beheerd door de CiscoWorks server of de Cisco Secure Access Control Server (ACS). Standaard beheert CiscoWorks verificatie en autorisatie, maar u kunt de tekst in Cisco Secure ACS wijzigen door de pagina AAA mode Setup in CiscoWorks Gemeenschappelijke services te gebruiken.

De belangrijkste voordelen van het gebruik van Cisco Secure ACS zijn de mogelijkheid om zeer granulaire gebruikersrollen te maken met gespecialiseerde permissies van toegangsrechten (bijvoorbeeld door de gebruiker in staat te stellen om bepaalde beleidstypen maar niet andere te configureren) en de mogelijkheid om gebruikers te beperken tot bepaalde apparaten door netwerkapparaatgroepen te configureren (NDGs).

De volgende onderwerpen beschrijven gebruikersrechten:

- Security Manager-toegangsrechten
- De betekenis van CiscoWorks-rollen
- De betekenis van Cisco Secure ACS-rollen
- Standaard associaties tussen toegangsrechten en rollen in Security Manager

Security Manager-toegangsrechten

Security Manager classificeert permissies in de categorieën zoals aangegeven:

1. **Bekijken** — Hiermee kunt u de huidige instellingen bekijken. Zie Toegangsrechten bekijken voor meer informatie.
2. **Wijzigen** — Hiermee kunt u de huidige instellingen wijzigen. Zie Toegangsrechten wijzigen voor meer informatie.
3. **Toewijzen** - staat u toe om beleid aan apparaten en de topologieën van VPN toe te wijzen. Zie Toestemmingen toewijzen voor meer informatie
4. **Goedkeuren**—Hiermee kunt u beleidswijzigingen en implementatiebanen goedkeuren. Zie Toestemmingen voor meer informatie goedkeuren.
5. **Importeren** - Hiermee kunt u de configuraties importeren die al op apparaten zijn geïmplementeerd in Security Manager.

6. **Hiermee kunt u** configuratie-wijzigingen in de apparaten in het netwerk **implementeren** en terugdraaiing uitvoeren om terug te keren naar een eerder ingevoerde configuratie.
7. **Controle**-staat u toe om bevelen aan apparaten uit te geven, zoals pingelen.
8. **Indienen**—hiermee kunt u uw configuratiewijzigingen ter goedkeuring voorleggen.

- Wanneer u permissies selecteert, toewijst, goedkeurt, importeert, controleert of implementeert, moet u ook de corresponderende recht van de mening selecteren; anders werkt Security Manager niet goed.
- Wanneer u beleidsrechten selecteert, moet u ook de betreffende toewijzen en weergeven.
- Wanneer u een beleid toestaat dat beleidsobjecten als deel van zijn definitie gebruikt, moet u ook weergaverechten aan deze objecttypes verlenen. Als u bijvoorbeeld de toestemming selecteert voor het wijzigen van routingbeleid, moet u ook de rechten selecteren voor het weergeven van netwerkobjecten en interfacerollen, die de objecttypes zijn die vereist zijn door het routeren van beleid.
- Hetzelfde geldt voor het toestaan van een object dat andere objecten gebruikt als onderdeel van de definitie. Als u bijvoorbeeld de toestemming selecteert voor het wijzigen van gebruikersgroepen, moet u ook de rechten selecteren voor het weergeven van netwerkobjecten, ACL-objecten en AAA servergroepen.

Toestemmingen bekijken

De weergave (alleen-lezen) toegangsrechten in Security Manager zijn verdeeld in de categorieën zoals getoond:

- Beleidstoegangsrechten bekijken
- Objecttoegangsrechten bekijken
- Aanvullende beeldtoegangsrechten

Beleidstoegangsrechten bekijken

Security Manager omvat de volgende weergaverechten voor beleid:

1. **Beeld > Beleid > Firewall.** Hiermee kunt u beleid voor firewallservice bekijken (in de beleidskeuzeknop onder Firewall) op PIX/ASA/FWSM-apparaten, IOS-routers en Catalyst 6500/7600 apparaten. Tot de voorbeelden van beleid van de firewallservice behoren toegangsregels, AAA-regels en inspectieregels.
2. **Beeld > Beleid > Inbraakpreventiesysteem.** Hiermee kunt u IPS-beleid bekijken (in de beleidsselector onder IPS), inclusief beleid voor IPS-ondersteuning die op IOS-routers wordt uitgevoerd.
3. **Beeld > Beleid > Afbeelding.** Hiermee kunt u een pakket voor de bijwerking van de handtekening selecteren in de wizard IPS-updates toepassen (bevindt zich onder Gereedschappen > IPS bijwerken), maar kunt u het pakket niet aan specifieke apparaten toewijzen, tenzij u ook de toestemming Wijzigen > Beleid > Afbeelding hebt.
4. **Beeld > Beleid > NAT**. Hier kunt u netwerkadresvertaalbeleid bekijken op PIX/ASA/FWSM-apparaten en IOS-routers. Voorbeelden van NAT-beleid zijn statische regels en dynamische regels.
5. **Beeld > Beleid > Site-to-Site VPN**. Hiermee kunt u site-to-site VPN-beleid bekijken op PIX/ASA/FWSM-apparaten, IOS-routers en Catalyst 6500/7600 apparaten. Voorbeelden van

site-to-site VPN-beleid zijn IKE-voorstellen, IPsec-voorstellen en vooraf gedeelde sleutels.

6. **Beeld > Beleid > VPN-toegang op afstand**. Hiermee kunt u VPN-beleid voor externe toegang bekijken op PIX/ASA/FWSM-apparaten, IOS-routers en Catalyst 6500/7600 apparaten. Voorbeelden van VPN-beleid voor externe toegang zijn IKE-voorstellen, IPsec-voorstellen en PKI-beleid.
7. **Beeld > Beleid > SSL VPN**. Hiermee kunt u SSL VPN-beleid op PIX/ASA/FWSM-apparaten en IOS-routers weergeven, zoals de SSL VPN-wizard.
8. **Beeld > Beleid > Interfaces**. Hiermee kunt u interfacebeleid (in de beleidsselector onder Interfaces) bekijken op PIX/ASA/FWSM-apparaten, IOS-routers, IPS-sensoren en Catalyst 6500/7600 apparaten.Op PIX/ASA/FWSM apparaten, bestrijkt deze toestemming hardwarepoorten en interface-instellingen.Op IOS routers, bestrijkt deze toestemming basisinstellingen en geavanceerde interfaceinstellingen, evenals ander interface-gerelateerd beleid, zoals DSL, PVC, PPP en dialerbeleid.Op IPS sensoren bestrijkt deze toestemming fysieke interfaces en samenvattende kaarten.Op Catalyst 6500/7600 apparaten, bestrijkt deze toestemming interfaces en instellingen van VLAN.
9. **Beeld > Beleid > Overbrugging**. Hiermee kunt u ARP-tabelbeleid weergeven (via de beleidsselector onder Platform > Bridging) op PIX/ASA/FWSM-apparaten.
10. **Beeld > Beleid > Apparaatbeheer**. Hiermee kunt u beleid voor apparaatbeheer (in de beleidskeuzeknop onder platform > apparaatbeheer) op PIX/ASA/FWSM-apparaten, IOS-routers en Catalyst 6500/7600-apparaten bekijken:Op PIX/ASA/FWSM apparaten, omvatten voorbeelden machine toegangsbeleid, server toegangsbeleid en overnamenbeleid.Op IOS routers omvatten voorbeelden apparatuur voor toegang (inclusief lijntoegangsbeleid), beleid voor servertoegang, AAA en Secure Apparatuur Provisioning.Op IPS sensoren heeft deze toestemming betrekking op het toegangsbeleid voor apparaten en het toegangsbeleid voor servers.Op Catalyst 6500/7600 apparaten, bestrijkt deze toestemming instellingen voor IDSM en toegangslijsten van VLAN.
11. **Beeld > Beleid > Identity**. Hiermee kunt u identiteitsbeleid (in de beleidskeuzeknop onder Platform > Identity) weergeven op Cisco IOS-routers, inclusief 802.1x- en netwerktoegangscontrole (NAC) beleid.
12. **Beeld > Beleid > Vastlegging**. Hiermee kunt u logbeleid (in de beleidskeuzeknop onder Platform > Logging) weergeven op PIX/ASA/FWSM-apparaten, IOS-routers en IPS-sensoren. Voorbeelden van logbeleid omvatten bloggінginstellingen, serverinstellingen en systeemserverbeleid.
13. **Beeld > Beleid > Multicast**. Hiermee kunt u multicast beleid (in de beleidsselector onder Platform > Multicast) op PIX/ASA/FWSM-apparaten bekijken. Voorbeelden van multicast beleid omvatten multicast routing en IGMP-beleid.
14. **Beeld > Beleid > QoS**. Hiermee kunt u QoS-beleid (in de beleidskeuzeknop onder Platform > Quality of Service) op Cisco IOS-routers bekijken.
15. **Beeld > Beleid > Routing**. Hiermee kunt u routingbeleid (in de beleidskeuzeknop onder Platform > Routing) bekijken op PIX/ASA/FWSM-apparaten en IOS-routers. Voorbeelden van routingbeleid omvatten OSPF, RIP, en statisch routeringsbeleid.
16. **Beeld > Beleid > Beveiliging**. Hiermee kunt u beveiligingsbeleid (in de beleidskeuzeknop onder Platform > Security) bekijken op PIX/ASA/FWSM-apparaten en IPS-sensoren:Op PIX/ASA/FWSM apparaten, omvat het veiligheidsbeleid anti-spoofing, fragment, en timeout instellingen.Op IPS-sensoren omvat het beveiligingsbeleid blokkeringsinstellingen.
17. **Beeld > Beleid > Regels voor het servicebeleid**. Hiermee kunt u beleid voor servicecontracten (in de beleidsselector onder Platform > Service Policy Rules) op PIX 7.x/ASA-apparaten bekijken. Voorbeelden zijn prioriteitswachtrijen en IPS, QoS en

verbindingsregels.

18. **Beeld > Beleid > Voorkeuren van gebruikers**. Hiermee kunt u het implementatiebeleid (in de beleidskeuzeknop onder Platform > Gebruikervoorkeuren) bekijken op PIX/ASA/FWSM-apparaten. Dit beleid bevat een optie voor het vereffenen van alle NAT-vertalingen bij de implementatie.
19. **Beeld > Beleid > Virtueel apparaat**. Hiermee kunt u virtueel sensorbeleid op IPS-apparaten bekijken. Dit beleid wordt gebruikt om virtuele sensoren te maken.
20. **Beeld > Beleid > FlexConfig**. Hiermee kunt u FlexConfiguration bekijken, dat is extra CLI-opdrachten en -instructies die kunnen worden uitgevoerd op PIX/ASA/FWSM-apparaten, IOS-routers en Catalyst 6500/7600-apparaten.

Objecttoegangsrechten bekijken

Security Manager omvat de volgende weergaverechten voor objecten:

1. **Beeld > Exemplaar > AAA servergroepen**. Hiermee kunt u AAA server group objecten bekijken. Deze objecten worden gebruikt in beleid dat AAA - diensten vereist (authenticatie, autorisatie en accounting).
2. **Beeld > Exemplaar > AAA servers**. Hiermee kunt u AAA-serverobjecten bekijken. Deze objecten vertegenwoordigen afzonderlijke AAA-servers die gedefinieerd zijn als deel van een AAA-servergroep.
3. **Beeld > Exemplaar > Toegangscontrolelijsten - standaard/uitgebreid**. Hier kunt u standaard- en uitgebreide ACL-objecten bekijken. Uitgebreide ACL-objecten worden gebruikt voor allerlei beleid, zoals NAT en NAC, en voor het instellen van VPN-toegang. Standaard ACL-objecten worden gebruikt voor dergelijk beleid zoals OSPF en SNMP en voor het instellen van VPN-toegang.
4. **Beeld > Objecten > Toegangscontrolelijsten** - Web. Hier kunt u web ACL-objecten bekijken. Web ACL-objecten worden gebruikt om contentfiltering uit te voeren in SSL VPN-beleid.
5. **Beeld > Exemplaar > ASA gebruikersgroepen**. Hiermee kunt u ASA gebruikersgroepobjecten bekijken. Deze objecten worden ingesteld op ASA security apparaten in Makkelijk VPN, externe VPN-toegang en SSL VPN-configuraties.
6. **Beeld > Objecten > Categorieën**. Hier kunt u categorieobjecten bekijken. Deze objecten helpen u regels en objecten in regeltabellen gemakkelijk te identificeren door het gebruik van kleur.
7. **Beeld > Objecten > Credentials**. Hiermee kunt u geloofsobjecten bekijken. Deze objecten worden gebruikt in de Makkelijk VPN-configuratie tijdens Uitgebreide IKE-verificatie (Xauth).
8. **Beeld > Objecten > FlexConfiguration**. Hiermee kunt u FlexConfig-objecten bekijken. Deze objecten, die configuratieopdrachten bevatten met extra instructies in de schrijftaal, kunnen worden gebruikt om opdrachten te configureren die niet worden ondersteund door de gebruikersinterface van Security Manager.
9. **Beeld > Exemplaar > IKE-voorstellen**. Hiermee kunt u IKE-objecten bekijken. Deze objecten bevatten de parameters die vereist zijn voor IKE-voorstellen in het VPN-beleid voor externe toegang.
10. **Beeld > Voorwerpen > Inspecteren - Class Maps** - DNS. Hiermee kunt u DNS-class kaartobjecten bekijken. Deze objecten passen DNS verkeer met specifieke criteria aan zodat de acties op dat verkeer kunnen worden uitgevoerd.
11. **Beeld > Exemplaar > Inspecteren - Klasse Maps - FTP**. Hiermee kunt u FTP class map objecten bekijken. Deze objecten passen het FTP verkeer aan met specifieke criteria zodat

de acties op dat verkeer kunnen worden uitgevoerd.

12. **Beeld > Exemplaar > Inspecteren - Klasse Maps - HTTP**. Hiermee kunt u HTTP class map objecten bekijken. Deze objecten passen HTTP verkeer aan met specifieke criteria zodat de handelingen op dat verkeer kunnen worden uitgevoerd.
13. **Beeld > Exemplaar > Inspecteren - Klasse Maps - IM**. Hiermee kunt u IM class map objecten bekijken. Deze objecten passen IM verkeer met specifieke criteria aan zodat op dat verkeer acties kunnen worden uitgevoerd.
14. **Beeld > Exemplaar > Inspecteren - Klasse Maps - SIP**. Hier kunt u SIP class map objecten bekijken. Deze objecten passen SIP verkeer met specifieke criteria aan zodat de acties op dat verkeer kunnen worden uitgevoerd.
15. **Beeld > Exemplaar > Inspecteren - beleidskaarten - DNS.** Hiermee kunt u DNS-beleidsobjecten bekijken. Deze objecten worden gebruikt om inspectiekaarten voor DNS-verkeer te maken.
16. **Beeld > Exemplaar > Bezoek - beleidskaarten - FTP.** Hier kunt u FTP-beleidsobjecten bekijken. Deze objecten worden gebruikt om inspectiekaarten te maken voor FTP-verkeer.
17. **Beeld > Exemplaar > Inspecteren - Beleidskaarten - GTP**. Hier kunt u GTP-beleidsobjecten bekijken. Deze objecten worden gebruikt om inspectiekaarten te maken voor GTP-verkeer.
18. **Beeld > Exemplaar > Inspecteren - Beleidskaarten - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Hiermee kunt u HTTP-beleidskaartobjecten bekijken die voor ASA/PIX 7.1.x-apparaten en IOS-routers zijn gemaakt. Deze objecten worden gebruikt om inspectiekaarten te maken voor HTTP-verkeer.
19. **Beeld > Exemplaar > Inspect - Policy Maps - HTTP (ASA7.2/PIX7.2)**. Hiermee kunt u HTTP-beleidskaartobjecten bekijken die voor ASA 7.2/PIX 7.2-apparaten zijn gemaakt. Deze objecten worden gebruikt om inspectiekaarten te maken voor HTTP-verkeer.
20. **Beeld > Exemplaar > Inspect - Policy Maps - IM (ASA7.2/PIX7.2)**. Hiermee kunt u IM beleid map objecten bekijken die voor ASA 7.2/PIX 7.2 apparaten zijn gemaakt. Deze objecten worden gebruikt om inspectiekaarten te maken voor IM-verkeer.
21. **Beeld > Exemplaar > Inspecteren - Beleidskaarten - IM (IOS)**. Hier kunt u IM beleidskaartobjecten bekijken die voor IOS-apparaten zijn gemaakt. Deze objecten worden gebruikt om inspectiekaarten te maken voor IM-verkeer.
22. **Beeld > Exemplaar > Inspecteren - Beleidskaarten - SIP**. Hier kunt u SIP-beleidsobjecten bekijken. Deze objecten worden gebruikt om inspectiekaarten voor SIP-verkeer te maken.
23. **Beeld > Exemplaar > Inspecteren - normale expressies**. Hier kunt u objecten met reguliere expressies bekijken. Deze objecten vertegenwoordigen individuele reguliere expressies die gedefinieerd worden als deel van een groep met reguliere expressies.
24. **Beeld > Exemplaar > Inspecteren - reguliere expressiegroepen**. Hier kunt u groepobjecten met reguliere expressies bekijken. Deze objecten worden door bepaalde class maps gebruikt en inspecteren kaarten om tekst in een pakket aan te passen.
25. **Beeld > Exemplaren > Inspecteren - TCP kaarten**. Hiermee kunt u TCP-kaartobjecten bekijken. Deze objecten aanpassen de inspectie op TCP in beide richtingen.
26. **Beeld > Objecten > Interfacetrollen**. Hier kunt u de interface-rolobjecten bekijken. Deze objecten definiëren naamgevingspatronen die meerdere interfaces op verschillende typen apparaten kunnen vertegenwoordigen. Interfacetrollen stellen u in staat om beleid op specifieke interfaces op meerdere apparaten toe te passen zonder de naam van elke interface handmatig te hoeven definiëren.
27. **Beeld > Objecten > IPsec transformatiesets**. Hiermee kunt u ingestelde objecten van IPsec omzetten. Deze objecten omvatten een combinatie van veiligheidsprotocollen, algoritmen en andere instellingen die precies specificeren hoe de gegevens in de IPsec-tunnel zullen

worden versleuteld en geauthentiseerd.

28. **Beeld > Exemplaren > Ldaf-kenmerken**. Hiermee kunt u lidaf-attribuut-objecten bekijken. Deze objecten worden gebruikt om aangepaste (door de gebruiker gedefinieerde) attribuennamen in kaart te brengen aan Cisco LDAP-eigennamen.
29. **Beeld > Exemplaren > netwerken/hosts**. Hiermee kunt u netwerk-/host-objecten bekijken. Deze objecten zijn logische collecties van IP adressen die netwerken, hosts of beide vertegenwoordigen. Network/host-objecten bieden u de mogelijkheid om beleid te definiëren zonder elk netwerk of elke host afzonderlijk te specificeren.
30. **Beeld > Objecten > PKI-inschrijvingen**. Hiermee kunt u PKI-inschrijvingsobjecten bekijken. Deze objecten definiëren de CA-servers (Certified Authority) die binnen een openbare sleutelinfrastructuur werken.
31. **Beeld > Exemplaar > lijst voor poortdoorsturen**. Hiermee kunt u de objecten van de poortverzendlijst bekijken. Deze objecten definiëren de mappingen van poortnummers op een verre client naar het IP-adres van de toepassing en poort achter een SSL VPN-poort.
32. **Beeld > Objecten > Secure-desktopconfiguraties**. Hiermee kunt u veilige desktop configuratie objecten bekijken. Deze objecten zijn herbruikbaar, genoemde componenten die door SSL VPN beleid kunnen worden geraadpleegd om een betrouwbare manier te bieden om alle sporen van gevoelige gegevens te elimineren die voor de duur van een SSL VPN-sessie worden gedeeld.
33. **Beeld > Exemplaar > Services - poortlijsten**. Hiermee kunt u objecten in de poortlijst bekijken. Deze objecten, die een of meer bereik van poortnummers bevatten, worden gebruikt om het proces van het maken van serviceobjecten te stroomlijnen.
34. **Beeld > Objecten > Services/Service Group** stelt u in staat om service- en servicegroep objecten te bekijken. Deze objecten zijn gedefinieerde afbeeldingen van protocol- en poortdefinities die netwerkservices beschrijven die door beleid worden gebruikt, zoals Kerberos, SSH en POP3.
35. **Beeld > Exemplaar > Enkele aanmelding op servers**. Hier kunt u één teken op serverobjecten bekijken. Single Sign-On (SSO) laat SSL VPN-gebruikers eenmaal een gebruikersnaam en wachtwoord invoeren en in staat zijn toegang te krijgen tot meerdere beschermde services en webservers.
36. **Beeld > Exemplaren > SLA monitoren**. Hier kunt u SLA-bewakingsobjecten bekijken. Deze objecten worden gebruikt door PIX/ASA security apparaten die versie 7.2 of later uitvoeren om route tracking uit te voeren. Deze eigenschap verstrekt een methode om de beschikbaarheid van een primaire route te volgen en een reserveroute te installeren als de primaire route mislukt.
37. **Beeld > Exemplaren > SSL VPN-aanpassingen**. Hier kunt u SSL VPN-aanpassingsobjecten bekijken. Deze objecten definiëren hoe de weergave van SSL VPN-pagina's die aan gebruikers worden weergegeven, zoals Login/Logout en Thuispagina's, moet worden gewijzigd.
38. **Beeld > Exemplaren > SSL VPN-gateways**. Hier kunt u SSL VPN-gateway-objecten bekijken. Deze objecten definiëren parameters die de gateway om als volmacht voor verbindingen aan de beschermde middelen in uw SSL VPN kunnen worden gebruikt.
39. **Beeld > Exemplaren > Stijlobjecten**. Hier kunt u stijlenobjecten bekijken. Met deze objecten kunt u stijlelementen, zoals lettertypekenmerken en kleuren, configureren om de verschijning van de SSL VPN-pagina die aan SSL VPN-gebruikers lijkt te worden aangepast wanneer ze verbinding maken met het security apparaat.
40. **Beeld > Objecten > Tekstobjecten**. Hier kunt u tekstobjecten in vrije vorm bekijken. Deze objecten omvatten een naam en waardepaar, waar de waarde één string, een lijst met

strings of een lijst met strings kan zijn.

41. **Beeld > Objecten > Tijdbereiken.** Hiermee kunt u objecten in het tijdbereik bekijken. Deze objecten worden gebruikt bij het maken van op tijd gebaseerde ACL's en inspectieregels. Ze worden ook gebruikt bij het definiëren van ASA-gebruikersgroepen om VPN-toegang tot specifieke tijden tijdens de week te beperken.
42. **Beeld > Exemplaar > verkeersstromen**. Hier kunt u verkeersstroomobjecten bekijken. Deze objecten definiëren specifieke verkeersstromen voor gebruik door PIX 7.x/ASA 7.x apparaten.
43. **Beeld > Voorwerpen > URL lijsten**. Hier kunt u URL-lijstobjecten bekijken. Deze objecten definiëren de URL's die op de portal pagina worden weergegeven na een succesvolle inlognaam. Dit stelt gebruikers in staat om toegang te hebben tot de middelen die op SSL VPN-websites beschikbaar zijn wanneer ze in de Clientloze toegangsmodus werken.
44. **Beeld > Objecten > Gebruikersgroepen**. Hier kunt u gebruikersgroepobjecten bekijken. Deze objecten definiëren groepen van verre cliënten die in Snelle VPN topologieën, verre toegang VPNs, en SSL VPNs worden gebruikt.
45. **Beeld > Objecten > WINS Server Lists**. Hiermee kunt u de WINS server list objecten bekijken. Deze objecten vertegenwoordigen WINS-servers, die door SSL VPN worden gebruikt om bestanden op externe systemen te openen of te delen.
46. **Beeld > Objecten > Interne - DN Regels**. Hiermee kunt u de DNA-regels bekijken die worden gebruikt door DNA-beleid. Dit is een intern object dat door Security Manager wordt gebruikt en dat niet in de Policy Object Manager voorkomt.
47. **Beeld > Exemplaar > interne - clientupdates**. Dit is een intern object dat door gebruikersgroepobjecten wordt vereist en dat niet in de Beleids Objectbeheer verschijnt.
48. **Beeld > Exemplaren > Interne - standaard ACE's**. Dit is een intern object voor de standaard toegangscontrolelijsten, die door ACL-objecten worden gebruikt.
49. **Beeld > Exemplaar > Interne uitgebreide ACE's.** Dit is een intern object voor uitgebreide toegangscontrole-items, die door ACL-objecten worden gebruikt.

Aanvullende beeldtoegangsrechten

Security Manager omvat de volgende extra weergaverechten:

1. **Beeld > Admin**. Hier kunt u beheerinstellingen voor Security Manager bekijken.
2. **Beeld > CLI**. Hiermee kunt u de CLI-opdrachten op een apparaat bekijken en de opdrachten bekijken die binnenkort worden uitgevoerd.
3. **Beeld > Archief van Config**. Hier kunt u de lijst weergeven van configuraties in het configuratiearchief. U kunt de apparaatconfiguratie of geen CLI-opdrachten bekijken.
4. **Beeld > Apparaten**. Hiermee kunt u apparaten in de apparaatweergave en alle bijbehorende informatie bekijken, inclusief de instellingen van het apparaat, eigenschappen, opdrachten enzovoort.
5. **Beeld > Apparaatbeheerders**. Hiermee kunt u alleen-lezen versies starten van de apparaatmanagers voor afzonderlijke apparaten, zoals Cisco Router en Security Devices Manager (DSM) voor Cisco IOS-routers.
6. **Beeld > Topologie**. Hier kunt u kaarten bekijken die in Kaart-weergave zijn ingesteld.

Wachttijden wijzigen

De (lees-schrijfrechten) rechten in Security Manager worden in de volgende categorieën verdeeld:

- Beleidsrechten wijzigen
- Objectrechten wijzigen
- Aanvullende wijzigingsrechten

Beleidsrechten wijzigen

Opmerking: Wanneer u beleidsrechten specificeert, zorg er dan voor dat u ook de betreffende toewijzen en weergeven van beleidsrechten hebt geselecteerd.

Security Manager bevat de volgende toegangsrechten voor beleid:

1. **Wijzigen > Beleid > Firewall**. Hiermee kunt u beleid voor firewallservice wijzigen (in de knop Policy onder Firewall) op PIX/ASA/FWSM-apparaten, IOS-routers en Catalyst 6500/7600-apparaten. Tot de voorbeelden van beleid van de firewallservice behoren toegangsregels, AAA-regels en inspectieregels.
2. **Wijzigen > Beleid > Inbraakpreventiesysteem**. Hiermee kunt u IPS-beleid wijzigen (in de knop Beleidsselectie onder IPS), inclusief beleid voor IPS-ondersteuning die op IOS-routers wordt uitgevoerd. Met deze toestemming kunt u ook handtekeningen afstemmen in de wizard Signature Update (Geldig onder Gereedschappen > Toepassen van IPS Update).
3. **Wijzigen > Beleid > Afbeelding**. Hiermee kunt u een pakket voor de bijwerking van de handtekening toewijzen aan apparaten in de wizard Toepassen van IPS-updates (onder Gereedschappen > Toepassen van IPS-update). Met deze toestemming kunt u ook auto-update instellingen aan specifieke apparaten toewijzen (onder Gereedschappen > Beveiligingsbeheer > IPS-updates).
4. **Wijzigen > Beleid > NAT**. Hier kunt u netwerkadresvertaalbeleid aanpassen op PIX/ASA/FWSM-apparaten en IOS-routers. Voorbeelden van NAT-beleid zijn statische regels en dynamische regels.
5. **Wijzigen > Beleid > Site-to-Site VPN**. Hiermee kunt u site-to-site VPN-beleid wijzigen op PIX/ASA/FWSM-apparaten, IOS-routers en Catalyst 6500/7600 apparaten. Voorbeelden van site-to-site VPN-beleid zijn IKE-voorstellen, IPsec-voorstellen en vooraf gedeelde sleutels.
6. **Wijzigen > Beleid > Externe Toegang VPN**. Hiermee kunt u beleid voor externe toegang van VPN wijzigen op PIX/ASA/FWSM-apparaten, IOS-routers en Catalyst 6500/7600 apparaten. Voorbeelden van VPN-beleid voor externe toegang zijn IKE-voorstellen, IPsec-voorstellen en PKI-beleid.
7. **Wijzigen > Beleid > SSL VPN**. Hiermee kunt u SSL VPN-beleid op PIX/ASA/FWSM-apparaten en IOS-routers wijzigen, zoals de SSL VPN-wizard.
8. **Wijzigen > Beleid > Interfaces**. Hiermee kunt u interfacebeleid wijzigen (in de beleidskeuzeknop onder Interfaces) op PIX/ASA/FWSM-apparaten, IOS-routers, IPS-sensoren en Catalyst 6500/7600-apparaten:Op PIX/ASA/FWSM apparaten, bestrijkt deze toestemming hardwarepoorten en interface-instellingen.Op IOS routers, bestrijkt deze toestemming basisinstellingen en geavanceerde interfaceinstellingen, evenals ander interface-gerelateerd beleid, zoals DSL, PVC, PPP en dialerbeleid.Op IPS sensoren bestrijkt deze toestemming fysieke interfaces en samenvattende kaarten.Op Catalyst 6500/7600 apparaten, bestrijkt deze toestemming interfaces en instellingen van VLAN.
9. **Wijzigen > Beleid > Overbrugging**. Hiermee kunt u ARP-tabelbeleid aanpassen (via de beleidsselector onder Platform > Bridging) op PIX/ASA/FWSM-apparaten.
10. **Wijzigen > Beleid > Apparaatbeheer**. Hiermee kunt u beleid voor apparaatbeheer wijzigen (in de beleidskeuzeknop onder platform > apparaatbeheer) op PIX/ASA/FWSM-apparaten,

IOS-routers en Catalyst 6500/7600-apparaten:Op PIX/ASA/FWSM apparaten, omvatten voorbeelden machine toegangsbeleid, server toegangsbeleid en overnamenbeleid.Op IOS routers omvatten voorbeelden apparatuur voor toegang (inclusief lijntoegangsbeleid), beleid voor servertoegang, AAA en Secure Apparatuur Provisioning.Op IPS sensoren heeft deze toestemming betrekking op het toegangsbeleid voor apparaten en het toegangsbeleid voor servers.Op Catalyst 6500/7600 apparaten, bestrijkt deze toestemming instellingen voor IDSM en de toegangslijst van VLAN.

11. **Wijzigen > Beleid > Identity**. Hiermee kunt u identiteitsbeleid wijzigen (in de beleidskeuzeknop onder Platform > Identity) op Cisco IOS-routers, inclusief 802.1x- en netwerktoegangscontrole (NAC) beleid.
12. **Wijzigen > Beleid > Vastlegging**. Hiermee kunt u logbeleid wijzigen (in de beleidskeuzeknop onder Platform > Logging) op PIX/ASA/FWSM-apparaten, IOS-routers en IPS-sensoren. Voorbeelden van logbeleid omvatten bloggінginstellingen, serverinstellingen en systeemserverbeleid.
13. **Wijzigen > Beleid > Multicast**. Hiermee kunt u multicast beleid aanpassen (in de beleidsselector onder Platform > Multicast) op PIX/ASA/FWSM-apparaten. Voorbeelden van multicast beleid omvatten multicast routing en IGMP-beleid.
14. **Wijzigen > Beleid > QoS**. Hiermee kunt u QoS-beleid wijzigen (in de beleidskeuzeknop onder Platform > Quality of Service) op Cisco IOS-routers.
15. **Wijzigen > Beleid > Routing**. Hiermee kunt u routingbeleid wijzigen (in de beleidskeuzeknop onder Platform > Routing) op PIX/ASA/FWSM-apparaten en IOS-routers. Voorbeelden van routingbeleid omvatten OSPF, RIP, en statisch routeringsbeleid.
16. **Wijzigen > Beleid > Beveiliging**. Hiermee kunt u beveiligingsbeleid wijzigen (in de beleidskeuzeknop onder Platform > Security) op PIX/ASA/FWSM-apparaten en IPS-sensoren:Op PIX/ASA/FWSM apparaten, omvat het veiligheidsbeleid anti-spoofing, fragment, en timeout instellingen.Op IPS-sensoren omvat het beveiligingsbeleid blokkeringsinstellingen.
17. **Wijzigen > Beleid > Regels voor het Servicebeleid**. Hiermee kunt u beleid voor serviceregel wijzigen (in de beleidsselector onder Platform > Service Policy Rules) op PIX 7.x/ASA-apparaten. Voorbeelden zijn prioriteitswachtrijen en IPS, QoS en verbindingsregels.
18. **Wijzigen > Beleid > Voorkeuren van gebruikers**. Hiermee kunt u het implementatiebeleid aanpassen (dat zich bevindt in de beleidskeuzeknop onder Platform > Gebruikervoorkeuren) op PIX/ASA/FWSM-apparaten. Dit beleid bevat een optie voor het vereffenen van alle NAT-vertalingen bij de implementatie.
19. **Wijzigen > Beleid > Virtueel apparaat**. Hiermee kunt u het beleid voor virtuele sensoren op IPS-apparaten wijzigen. Gebruik dit beleid om virtuele sensoren te maken.
20. **Wijzigen > Beleid > FlexConfig**. Hiermee kunt u FlexConfigureert, wat extra CLI-opdrachten en -instructies zijn die kunnen worden uitgevoerd op PIX/ASA/FWSM-apparaten, IOS-routers en Catalyst 6500/7600-apparaten.

Objectrechten wijzigen

Security Manager omvat de volgende weergaverechten voor objecten:

1. **Wijzigen > Exemplaar > AAA servergroepen**. Hiermee kunt u AAA server group objecten bekijken. Deze objecten worden gebruikt in beleid dat AAA - diensten vereist (authenticatie, autorisatie en accounting).
2. **Wijzigen > Objecten > AAA-servers**. Hiermee kunt u AAA-serverobjecten bekijken. Deze

objecten vertegenwoordigen afzonderlijke AAA-servers die gedefinieerd zijn als deel van een AAA-servergroep.

3. **Wijzigen > Exemplaar > Toegangscontrolelijsten - standaard/uitgebreid**. Hier kunt u standaard- en uitgebreide ACL-objecten bekijken. Uitgebreide ACL-objecten worden gebruikt voor allerlei beleid, zoals NAT en NAC, en voor het instellen van VPN-toegang. Standaard ACL-objecten worden gebruikt voor dergelijk beleid zoals OSPF en SNMP en voor het instellen van VPN-toegang.
4. **Wijzigen > Objecten > Toegangscontrolelijsten - Web**. Hier kunt u web ACL-objecten bekijken. Web ACL-objecten worden gebruikt om contentfiltering uit te voeren in SSL VPN-beleid.
5. **Wijzigen > Exemplaar > ASA** gebruikersgroepen. Hiermee kunt u ASA gebruikersgroepobjecten bekijken. Deze objecten worden ingesteld op ASA security apparaten in Makkelijk VPN, externe VPN-toegang en SSL VPN-configuraties.
6. **Wijzigen > Objecten > Categorieën**. Hier kunt u categorieobjecten bekijken. Deze objecten helpen u regels en objecten in regeltabellen gemakkelijk te identificeren door het gebruik van kleur.
7. **Wijzigen > Objecten > Credentials**. Hiermee kunt u geloofsobjecten bekijken. Deze objecten worden gebruikt in de Makkelijk VPN-configuratie tijdens Uitgebreide IKE-verificatie (Xauth).
8. **Wijzigen > Objecten > FlexConfiguration**. Hiermee kunt u FlexConfig-objecten bekijken. Deze objecten, die configuratieopdrachten bevatten met extra instructies in de schrijftaal, kunnen worden gebruikt om opdrachten te configureren die niet worden ondersteund door de gebruikersinterface van Security Manager.
9. **Wijzigen > Exemplaar > IKE-voorstellen**. Hiermee kunt u IKE-objecten bekijken. Deze objecten bevatten de parameters die vereist zijn voor IKE-voorstellen in het VPN-beleid voor externe toegang.
10. **Wijzigen > Exemplaar > Inspecteren - Klasse Maps - DNS**. Hiermee kunt u DNS-class kaartobjecten bekijken. Deze objecten passen DNS verkeer met specifieke criteria aan zodat de acties op dat verkeer kunnen worden uitgevoerd.
11. **Wijzigen > Exemplaar > Inspecteren - Klasse Maps - FTP**. Hiermee kunt u FTP class map objecten bekijken. Deze objecten passen het FTP verkeer aan met specifieke criteria zodat de acties op dat verkeer kunnen worden uitgevoerd.
12. **Wijzigen > Exemplaar > Inspecteren - Klasse Maps - HTTP**. Hiermee kunt u HTTP class map objecten bekijken. Deze objecten passen HTTP verkeer aan met specifieke criteria zodat de handelingen op dat verkeer kunnen worden uitgevoerd.
13. **Wijzigen > Exemplaar > Inspecteren - Klasse Maps - IM**. Hiermee kunt u IM class map objecten bekijken. Deze objecten passen IM verkeer met specifieke criteria aan zodat op dat verkeer acties kunnen worden uitgevoerd.
14. **Wijzigen > Exemplaar > Inspecteren - Klasse Maps - SIP**. Hier kunt u SIP class map objecten bekijken. Deze objecten passen SIP verkeer met specifieke criteria aan zodat de acties op dat verkeer kunnen worden uitgevoerd.
15. **Wijzigen > Exemplaar > Inspecteren - Beleidskaarten - DNS**. Hiermee kunt u DNS-beleidsobjecten bekijken. Deze objecten worden gebruikt om inspectiekaarten voor DNS-verkeer te maken.
16. **Wijzigen > Exemplaar > Inspecteren - beleidskaarten - FTP**. Hier kunt u FTP-beleidsobjecten bekijken. Deze objecten worden gebruikt om inspectiekaarten te maken voor FTP-verkeer.
17. **Wijzigen > Exemplaar > Inspecteren - Beleidskaarten - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Hiermee kunt u HTTP-beleidskaartobjecten bekijken die voor ASA/PIX 7.x-apparaten en

IOS-routers zijn gemaakt. Deze objecten worden gebruikt om inspectiekaarten te maken voor HTTP-verkeer.

18. **Wijzigen > Exemplaar > Inspecteren - Beleidskaarten - HTTP (ASA7.2/PIX7.2)**. Hiermee kunt u HTTP-beleidskaartobjecten bekijken die voor ASA 7.2/PIX 7.2-apparaten zijn gemaakt. Deze objecten worden gebruikt om inspectiekaarten te maken voor HTTP-verkeer.
19. **Wijzigen > Exemplaar > Inspecteren - Beleidskaarten - IM (ASA7.2/PIX7.2)**. Hiermee kunt u IM beleid map objecten bekijken die voor ASA 7.2/PIX 7.2 apparaten zijn gemaakt. Deze objecten worden gebruikt om inspectiekaarten te maken voor IM-verkeer.
20. **Wijzigen > Exemplaar > Inspecteren - Beleidskaarten - IM (IOS)**. Hier kunt u IM beleidskaartobjecten bekijken die voor IOS-apparaten zijn gemaakt. Deze objecten worden gebruikt om inspectiekaarten te maken voor IM-verkeer.
21. **Wijzigen > Exemplaar > Inspecteren - beleidskaarten - SIP**. Hier kunt u SIP-beleidsobjecten bekijken. Deze objecten worden gebruikt om inspectiekaarten voor SIP-verkeer te maken.
22. **Wijzigen > Exemplaar > Inspecteren - reguliere expressies**. Hier kunt u objecten met reguliere expressies bekijken. Deze objecten vertegenwoordigen individuele reguliere expressies die gedefinieerd worden als deel van een groep met reguliere expressies.
23. **Wijzigen > Objecten > Inspecteren - Reguliere expressiegroepen**. Hier kunt u groepobjecten met reguliere expressies bekijken. Deze objecten worden door bepaalde class maps gebruikt en inspecteren kaarten om tekst in een pakket aan te passen.
24. **Wijzigen > Exemplaar > Inspecteren - TCP kaarten**. Hiermee kunt u TCP-kaartobjecten bekijken. Deze objecten aanpassen de inspectie op TCP in beide richtingen.
25. **Wijzigen > Objecten > Interfacetrollen**. Hier kunt u de interface-rolobjecten bekijken. Deze objecten definiëren naamgevingspatronen die meerdere interfaces op verschillende typen apparaten kunnen vertegenwoordigen. Interfacetrollen stellen u in staat om beleid op specifieke interfaces op meerdere apparaten toe te passen zonder de naam van elke interface handmatig te hoeven definiëren.
26. **Wijzigen > Objecten > IPsec Transformatiesets**. Hiermee kunt u ingestelde objecten van IPsec omzetten. Deze objecten omvatten een combinatie van veiligheidsprotocollen, algoritmen en andere instellingen die precies specificeren hoe de gegevens in de IPsec-tunnel zullen worden versleuteld en geauthentiseerd.
27. **Wijzigen > Exemplaren > Ldaf-kenmerken**. Hiermee kunt u lidaf-attribuut-objecten bekijken. Deze objecten worden gebruikt om aangepaste (door de gebruiker gedefinieerde) attribuennamen in kaart te brengen aan Cisco LDAP-eigennamen.
28. **Wijzigen > Objecten > Netwerken/hosts**. Hiermee kunt u netwerk-/host-objecten bekijken. Deze objecten zijn logische collecties van IP adressen die netwerken, hosts of beide vertegenwoordigen. Network/host-objecten bieden u de mogelijkheid om beleid te definiëren zonder elk netwerk of elke host afzonderlijk te specificeren.
29. **Wijzigen > Objecten > PKI-inschrijvingen**. Hiermee kunt u PKI-inschrijvingsobjecten bekijken. Deze objecten definiëren de CA-servers (Certified Authority) die binnen een openbare sleutelinfrastructuur werken.
30. **Wijzigen > Exemplaar > lijst met poortdoorsturen**. Hiermee kunt u de objecten van de poortverzendlijst bekijken. Deze objecten definiëren de mappingen van poortnummers op een verre client naar het IP-adres van de toepassing en poort achter een SSL VPN-poort.
31. **Wijzigen > Objecten > Beveiligde desktopconfiguraties**. Hiermee kunt u veilige desktop configuratie objecten bekijken. Deze objecten zijn herbruikbaar, genoemde componenten die door SSL VPN beleid kunnen worden geraadpleegd om een betrouwbare manier te bieden om alle sporen van gevoelige gegevens te elimineren die voor de duur van een SSL

VPN-sessie worden gedeeld.

32. **Wijzigen > Exemplaar > Services - poortlijsten**. Hiermee kunt u objecten in de poortlijst bekijken. Deze objecten, die een of meer bereik van poortnummers bevatten, worden gebruikt om het proces van het maken van serviceobjecten te stroomlijnen.
33. **Wijzigen > Exemplaren > Services/servicegroepen.** Hier kunt u de service- en servicegroep objecten bekijken. Deze objecten zijn gedefinieerde afbeeldingen van protocol- en poortdefinities die netwerkservices beschrijven die door beleid worden gebruikt, zoals Kerberos, SSH en POP3.
34. **Wijzigen > Exemplaar > Eenvoudig aanmelding op servers.** Hier kunt u één teken op serverobjecten bekijken. Single Sign-On (SSO) laat SSL VPN-gebruikers eenmaal een gebruikersnaam en wachtwoord invoeren en in staat zijn toegang te krijgen tot meerdere beschermde services en webservers.
35. **Wijzigen > Exemplaar > SLA monitoren**. Hier kunt u SLA-bewakingsobjecten bekijken. Deze objecten worden gebruikt door PIX/ASA security apparaten die versie 7.2 of later uitvoeren om route tracking uit te voeren. Deze eigenschap verstrekt een methode om de beschikbaarheid van een primaire route te volgen en een reserveroute te installeren als de primaire route mislukt.
36. **Wijzigen > Objecten > SSL VPN-aanpassingen**. Hier kunt u SSL VPN-aanpassingsobjecten bekijken. Deze objecten definiëren hoe de weergave van SSL VPN-pagina's die aan gebruikers worden weergegeven, zoals Login/Logout en Thuispagina's, moet worden gewijzigd.
37. **Wijzigen > Objecten > SSL VPN-gateways**. Hier kunt u SSL VPN-gateway-objecten bekijken. Deze objecten definiëren parameters die de gateway om als volmacht voor verbindingen aan de beschermde middelen in uw SSL VPN kunnen worden gebruikt.
38. **Wijzigen > Objecten > Stijlobjecten**. Hier kunt u stijlenobjecten bekijken. Met deze objecten kunt u stijlelementen, zoals lettertypekenmerken en kleuren, configureren om de verschijning van de SSL VPN-pagina die aan SSL VPN-gebruikers lijkt te worden aangepast wanneer ze verbinding maken met het security apparaat.
39. **Wijzigen > Objecten > Tekstobjecten**. Hier kunt u tekstobjecten in vrije vorm bekijken. Deze objecten omvatten een naam en waardepaar, waar de waarde één string, een lijst met strings of een lijst met strings kan zijn.
40. **Wijzigen > Objecten > Tijdbereiken.** Hiermee kunt u objecten in het tijdbereik bekijken. Deze objecten worden gebruikt bij het maken van op tijd gebaseerde ACL's en inspectieregels. Ze worden ook gebruikt bij het definiëren van ASA-gebruikersgroepen om VPN-toegang tot specifieke tijden tijdens de week te beperken.
41. **Wijzigen > Exemplaar > verkeersstromen**. Hier kunt u verkeersstroomobjecten bekijken. Deze objecten definiëren specifieke verkeersstromen voor gebruik door PIX 7.x/ASA 7.x apparaten.
42. **Wijzigen > Exemplaren > URL lijsten**. Hier kunt u URL-lijstobjecten bekijken. Deze objecten definiëren de URL's die op de portal pagina worden weergegeven na een succesvolle inlognaam. Dit stelt gebruikers in staat om toegang te hebben tot de middelen die op SSL VPN-websites beschikbaar zijn wanneer ze in de Clientloze toegangsmodus werken.
43. **Wijzigen > Objecten > Gebruikersgroepen**. Hier kunt u gebruikersgroepobjecten bekijken. Deze objecten definiëren groepen van externe cliënten die in Snelle VPN-topologieën, externe VPN's en SSL VPN's worden gebruikt
44. **Wijzigen > Objecten > WINS Server Lists**. Hiermee kunt u de WINS server list objecten bekijken. Deze objecten vertegenwoordigen WINS-servers, die door SSL VPN worden gebruikt om bestanden op externe systemen te openen of te delen.

45. **Wijzigen > Objecten > Interne - DN - regels.** Hiermee kunt u de DNA-regels bekijken die worden gebruikt door DNA-beleid. Dit is een intern object dat door Security Manager wordt gebruikt en dat niet in de Policy Object Manager voorkomt.
46. **Wijzigen > Exemplaar > interne - clientupdates**. Dit is een intern object dat door gebruikersgroepobjecten wordt vereist en dat niet in de Beleids Objectbeheer verschijnt.
47. **Wijzigen > Exemplaren > Interne - standaard ACE**. Dit is een intern object voor de standaard toegangscontrolelijsten, die door ACL-objecten worden gebruikt.
48. **Wijzigen > Exemplaar > Intern - uitgebreid ACE**. Dit is een intern object voor uitgebreide toegangscontrole-items, die door ACL-objecten worden gebruikt.

Aanvullende wijzigingsrechten

Security Manager bevat de extra rechten voor het wijzigen van de rechten zoals weergegeven:

1. **Wijzigen > Admin**. Hiermee kunt u beheerinstellingen voor Security Manager wijzigen.
2. **Wijzigen > Config**. Hiermee kunt u de configuratie van het apparaat wijzigen in het Configuratiearchiefbestand. Daarnaast kunt u configuraties aan het archief toevoegen en het Configuratiearchiefgereedschap aanpassen.
3. **Wijzigen > Apparaten**. Hiermee kunt u apparaten toevoegen en verwijderen en eigenschappen van het apparaat wijzigen. Om het beleid op het apparaat te ontdekken dat wordt toegevoegd, moet u ook de Toestemming van de Invoer toestaan. Als u bovendien de toestemming van Wijzigen > Apparaten toelaat, zorg ervoor dat u ook het Toewijzen > Beleid > de toestemming van Interfaces toelaat.
4. **Wijzigen > Hierarchy**. Hiermee kunt u apparaatgroepen wijzigen.
5. **Wijzigen > Topologie**. Hier kunt u kaarten in de Kaart-weergave wijzigen.

Toewijzing van toegangsrechten

Security Manager omvat de beleidstoewijzing zoals getoond:

1. **Toewijzen > Beleid > Firewall**. Hiermee kunt u beleid voor firewallservice (in de beleidsselector onder Firewall) toewijzen aan PIX/ASA/FWSM-apparaten, IOS-routers en Catalyst 6500/7600-apparaten. Tot de voorbeelden van beleid van de firewallservice behoren toegangsregels, AAA-regels en inspectieregels.
2. **Toewijzen > Beleid > Inbraakpreventiesysteem**. Hiermee kunt u IPS-beleid toewijzen (in de beleidskeuzeknop onder IPS), inclusief beleid voor IPS-ondersteuning die op IOS-routers wordt uitgevoerd.
3. **Toewijzen > Beleid > Afbeelding**. Deze toestemming wordt momenteel niet gebruikt door Security Manager.
4. **Toewijzen > Beleid > NAT**. Hiermee kunt u netwerkadresvertaalbeleid toewijzen aan PIX/ASA/FWSM-apparaten en IOS-routers. Voorbeelden van NAT-beleid zijn statische regels en dynamische regels.
5. **Toewijzen > Beleid > Site-to-Site VPN**. Hiermee kunt u site-to-site VPN-beleid toewijzen aan PIX/ASA/FWSM-apparaten, IOS-routers en Catalyst 6500/7600 apparaten. Voorbeelden van site-to-site VPN-beleid zijn IKE-voorstellen, IPsec-voorstellen en vooraf gedeelde sleutels.
6. **Toewijzen > Beleid > Externe Toegang VPN**. Hiermee kunt u VPN-beleid voor externe toegang toewijzen aan PIX/ASA/FWSM-apparaten, IOS-routers en Catalyst 6500/7600 apparaten. Voorbeelden van VPN-beleid voor externe toegang zijn IKE-voorstellen, IPsec-

voorstellen en PKI-beleid.

7. **Toewijzen > Beleid > SSL VPN**. Hiermee kunt u SSL VPN-beleid toewijzen aan PIX-/ASA/FWSM-apparaten en IOS-routers, zoals de SSL VPN-wizard.
8. **Toewijzen > Beleid > Interfaces**. Hiermee kunt u interfacebeleid (in de beleidsselector onder Interfaces) toewijzen aan PIX/ASA/FWSM-apparaten, IOS-routers en Catalyst 6500/7600-apparaten:Op PIX/ASA/FWSM apparaten, bestrijkt deze toestemming hardwarepoorten en interface-instellingen.Op IOS routers, bestrijkt deze toestemming basisinstellingen en geavanceerde interfaceinstellingen, evenals ander interface-gerelateerd beleid, zoals DSL, PVC, PPP en dialerbeleid.Op Catalyst 6500/7600 apparaten, bestrijkt deze toestemming interfaces en instellingen van VLAN.
9. **Toewijzen > Beleid > Overbrugging**. Hiermee kunt u ARP-tabelbeleid (in de beleidsselector onder Platform > Bridging) toewijzen aan PIX/ASA/FWSM-apparaten.
10. **Toewijzen > Beleid > Apparaatbeheer**. Hiermee kunt u beleid voor apparaatbeheer (in de beleidskeuzeknop onder platform > apparaatbeheer) toewijzen aan PIX/ASA/FWSM-apparaten, IOS-routers en Catalyst 6500/7600-apparaten:Op PIX/ASA/FWSM apparaten, omvatten voorbeelden machine toegangsbeleid, server toegangsbeleid en overnamenbeleid.Op IOS routers omvatten voorbeelden apparatuur voor toegang (inclusief lijntoegangsbeleid), beleid voor servertoegang, AAA en Secure Apparatuur Provisioning.Op IPS sensoren heeft deze toestemming betrekking op het toegangsbeleid voor apparaten en het toegangsbeleid voor servers.Op Catalyst 6500/7600 apparaten, bestrijkt deze toestemming instellingen voor IDSM en toegangslijsten van VLAN.
11. **Toewijzen > Beleid > Identity**. Hiermee kunt u identiteitsbeleid (in de beleidskeuzeknop onder Platform > Identity) toewijzen aan Cisco IOS-routers, inclusief 802.1x- en netwerktoegangscontrole (NAC) beleid.
12. **Toewijzen > Beleid > Vastlegging**. Hiermee kunt u logbeleid (in de beleidskeuzeknop onder Platform > Logging) toewijzen aan PIX/ASA/FWSM apparaten en IOS-routers. Voorbeelden van logbeleid omvatten blogginginstellingen, serverinstellingen en systeemserverbeleid.
13. **Toewijzen > Beleid > Multicast**. Hiermee kunt u multicast beleid (in de beleidsselector onder Platform > Multicast) toewijzen aan PIX/ASA/FWSM-apparaten. Voorbeelden van multicast beleid omvatten multicast routing en IGMP-beleid.
14. **Toewijzen > Beleid > QoS**. Hiermee kunt u QoS-beleid (in de beleidskeuzeknop onder Platform > Quality of Service) aan Cisco IOS-routers toewijzen.
15. **Toewijzen > Beleid > Routing**. Hiermee kunt u routingbeleid (in de beleidskeuzeknop onder Platform > Routing) toewijzen aan PIX/ASA/FWSM-apparaten en IOS-routers. Voorbeelden van routingbeleid omvatten OSPF, RIP, en statisch routeringsbeleid.
16. **Toewijzen > Beleid > Veiligheid**. Hiermee kunt u beveiligingsbeleid (in de beleidskeuzeknop onder Platform > Security) toewijzen aan PIX/ASA/FWSM-apparaten. Het veiligheidsbeleid omvat anti-spoofing, fragment, en time-out instellingen.
17. **Toewijzen > Beleid > Regels voor het dienstenbeleid**. Hiermee kunt u beleid voor serviceregel toewijzen (in de beleidsselector onder Platform > Service Policy Rules) aan PIX 7.x/ASA-apparaten. Voorbeelden zijn prioriteitswachtrijen en IPS, QoS en verbindingsregels.
18. **Toewijzen > Beleid > Voorkeuren van gebruikers**. Hiermee kunt u het implementatiebeleid (in de beleidskeuzeknop onder Platform > Gebruikervoorkeuren) toewijzen aan PIX/ASA/FWSM-apparaten. Dit beleid bevat een optie voor het vereffenen van alle NAT-vertalingen bij de implementatie.
19. **Toewijzen > Beleid > Virtueel apparaat**. Hiermee kunt u virtueel sensorbeleid aan IPS-apparaten toewijzen. Gebruik dit beleid om virtuele sensoren te maken.

20. **Toewijzen > Beleid > FlexConfig**. Hiermee kunt u FlexConfiguration toewijzen, dat wil zeggen extra CLI-opdrachten en -instructies die kunnen worden uitgevoerd op PIX/ASA/FWSM-apparaten, IOS-routers en Catalyst 6500/7600-apparaten.

Opmerking: Wanneer u toebevoorstellingen specificeert, zorg er dan voor dat u ook de corresponderende weergaverechten hebt geselecteerd.

Toestemmingen goedkeuren

Security Manager geeft de goedkeuring van rechten zoals getoond:

1. **Goedkeuren > CLI**. Hier kunt u de CLI-opdrachtwijzigingen goedkeuren die in een invoertaak zijn opgenomen.
2. **Goedkeuren > Beleid**. Hiermee kunt u de configuratiewijzigingen in het beleid goedkeuren die zijn uitgevoerd in een werkstroomactiviteit.

De betekenis van CiscoWorks-rollen

Wanneer de gebruikers in de Gemeenschappelijke Diensten van CiscoWorks worden gecreëerd, worden zij toegewezen één of meerdere rollen. De permissies die bij elke rol zijn gekoppeld, bepalen de bewerkingen die elke gebruiker mag uitvoeren in Security Manager.

De volgende onderwerpen beschrijven de rollen van CiscoWorks:

- CiscoWorks standaardrollen voor normale services
- Rollen toewijzen aan gebruikers in CiscoWorks Gemeenschappelijke services

CiscoWorks standaardrollen voor normale services

CiscoWorks Common Services bevat de volgende standaardrollen:

1. Gebruikers **van Help**-helpdesk kunnen apparaten, beleid, objecten en topologiekaarten bekijken (maar niet wijzigen).
2. **Netwerkoperator**-Naast weergave van de rechten kunnen netwerkoperatoren CLI-opdrachten en beheerinstellingen voor Security Manager bekijken. Netwerkbeheerders kunnen ook de opdrachten voor het configuratie-archief en de configuratie-indeling (zoals ping) aan apparaten aanpassen.
3. **Approver**-Naast weergave van de machtigingen, kunnen de accepteerders implementatiebanen goedkeuren of afwijzen. Ze kunnen geen plaatsing uitvoeren.
4. **Netwerkbeheerder**—De netwerkbeheerders hebben volledige weergave en wijzig rechten, behalve voor het wijzigen van beheerinstellingen. Ze kunnen apparaten en het beleid ontdekken dat op deze apparaten is ingesteld, beleid aan apparaten toewijzen en opdrachten aan apparaten uitgeven. Netwerkbeheerders kunnen geen activiteiten of implementatiebanen goedkeuren; zij kunnen echter wel banen inzetten die door anderen zijn goedgekeurd .
5. **Systeembeheerder**— systeembeheerders hebben volledige toegang tot alle security Manager rechten, waaronder wijziging, beleidstoewijzing, activiteit en taakgoedkeuring, ontdekking, implementatie en het uitgeven van opdrachten aan apparaten.

Opmerking: Aanvullende rollen, zoals exportgegevens, kunnen in Common Services worden

weergegeven als er extra toepassingen op de server worden geïnstalleerd. De rol van exportgegevens is bestemd voor ontwikkelaars van derden en wordt niet gebruikt door Security Manager.

Tip: Hoewel u de definitie van CiscoWorks rollen niet kunt wijzigen, kunt u definiëren welke rollen aan elke gebruiker worden toegewezen. Voor meer informatie, zie Rollen aan gebruikers in de Gemeenschappelijke Diensten van CiscoWorks toewijzen.

Rollen toewijzen aan gebruikers in CiscoWorks Gemeenschappelijke services

Met CiscoWorks Common Services kunt u bepalen welke rollen aan elke gebruiker zijn toegewezen. Door de roldefinitie voor een gebruiker te wijzigen, wijzigt u de soorten bewerkingen die deze gebruiker in Security Manager mag uitvoeren. Als u bijvoorbeeld de rol van het Help-bureaublad toewijst, is de gebruiker beperkt tot weergavebewerkingen en kan u geen gegevens wijzigen. Als u echter de rol van netwerkoperator toewijst, kan de gebruiker ook het configuratiearchief wijzigen. U kunt meerdere rollen toewijzen aan elke gebruiker.

Opmerking: U moet Security Manager opnieuw opstarten nadat u wijzigingen in de gebruikersrechten hebt aangebracht.

Procedure: Initiatief

1. Selecteer in Common Services de optie **Server > Security** en selecteer vervolgens **Single-Server Trust Management > Local User Setup** vanuit het TOC-gedeelte.**Tip:** Als u de pagina Local User Setup wilt bereiken vanuit Security Manager, selecteert u Gereedschappen > Security Manager Management > Server Security en vervolgens klikt u op Local User Setup.
2. Selecteer het aanvinkvakje naast een bestaande gebruiker en klik vervolgens op **Bewerken**.
3. Selecteer in de pagina met gebruikersinformatie de rollen die u aan deze gebruiker wilt toewijzen door op de selectievakjes in te klikken.Voor meer informatie over elke rol, zie CiscoWorks Standaard services rol.
4. Klik op **OK** om de wijzigingen op te slaan.
5. Start Security Manager opnieuw.

De betekenis van Cisco Secure ACS-rollen

Cisco Secure ACS biedt grotere flexibiliteit voor het beheer van security Manager rechten dan CiscoWorks omdat het toepassingsspecifieke rollen ondersteunt die u kunt configureren. Elke rol bestaat uit een reeks machtigingen die het niveau van de autorisatie aan Security Manager-taken bepalen. In Cisco Secure ACS, kent u een rol toe aan elke gebruikersgroep (en optioneel ook aan individuele gebruikers), die elke gebruiker in die groep in staat stelt om de bewerkingen uit te voeren die zijn toegestaan door de permissies die voor die rol zijn gedefinieerd.

Daarnaast kunt u deze rollen toewijzen aan Cisco Secure ACS-apparaatgroepen, zodat permissies op verschillende sets apparaten kunnen worden gedifferentieerd.

Opmerking: Cisco Secure ACS-apparaatgroepen zijn onafhankelijk van Security Manager-apparaatgroepen.

De volgende onderwerpen beschrijven Cisco Secure ACS-rollen:

Cisco beveiligde ACS-standaardrollen

Cisco Secure ACS omvat de zelfde rollen als CiscoWorks (zie het begrijpen van CiscoWorks Roles), plus deze extra rollen:

1. **Security Approver**-Security benaderingen kunnen apparaten, beleid, objecten, kaarten, CLI opdrachten en beheerinstellingen bekijken (maar niet wijzigen). Bovendien kunnen de veiligheidsbeheerders de configuratiewijzigingen in een activiteit goedkeuren of afwijzen. Ze kunnen de stationeringsbaan niet goedkeuren of afwijzen en ze kunnen ook geen inzet uitvoeren.
2. **Beveiligingsbeheerder** - Naast het hebben van ViewBorders kunnen de beheerders apparaten, apparaatgroepen, beleid, objecten en topologiekaarten wijzigen. Ze kunnen ook beleid aan apparaten en de topologieën van VPN toewijzen en ontdekking uitvoeren om nieuwe apparaten in het systeem in te voeren.
3. **Netwerkbeheerder** - Naast de weergave van de toegangsrechten kunnen de netwerkbeheerders het configuratiearchief wijzigen, implementaties uitvoeren en opdrachten naar apparaten uitgeven.

Opmerking: de rechten in de Cisco Secure ACS-netwerkbeheerrol zijn anders dan die in de CiscoWorks-netwerkbeheerrol. Zie De rol van CiscoWorks begrijpen voor meer informatie.

In tegenstelling tot Cisco Secure ACS stelt u in staat om de rechten aan te passen die aan elke Security Manager-rol zijn gekoppeld. Voor meer informatie over het wijzigen van de standaardrollen, zie het Aanpassen van Cisco Secure ACS Roles.

Opmerking: Cisco Secure ACS 3.3 of hoger moet voor Security Manager toestemming zijn geïnstalleerd.

Cisco beveiligde ACS-rollen aanpassen

Cisco Secure ACS stelt u in staat de rechten aan te passen die aan elke Security Manager-rol zijn gekoppeld. U kunt Cisco Secure ACS ook aanpassen door speciale gebruikersrollen te maken met rechten die op bepaalde Security Manager-taken zijn gericht.

Opmerking: U moet Security Manager opnieuw opstarten nadat u wijzigingen in de gebruikersrechten hebt aangebracht.

Procedure: Initiatief

1. Klik in Cisco Secure ACS op **Shared Profile Componenten** op de navigatiebalk.
2. Klik op **Cisco Security Manager** op de pagina Gedeelde componenten. De rollen die voor Security Manager zijn ingesteld worden weergegeven.
3. Voer een van de volgende handelingen uit:Klik op **Toevoegen** om een rol te maken. Ga naar stap 4.Als u een bestaande rol wilt wijzigen, klikt u op de rol. Ga naar stap 5.
4. Voer een naam in voor de rol en, optioneel, een beschrijving.
5. Selecteer en deselecteer de vinkjes van de permissies boom om de permissies voor deze rol te definiërenDoor het aanvinkvakje voor een tak van de boom te selecteren, worden alle

rechten in die tak geselecteerd. Bijvoorbeeld, selecteert het selecteren van **Toewijzen** al de toegewezen machtigingen.Zie Security Manager-toegangsrechten voor een volledige lijst met Security Manager.**Opmerking:** Wanneer u rechten selecteert die worden aangepast, goedgekeurd, toegewezen, geïmporteerd, gecontroleerd of ingezet, moet u ook de corresponderende weergaverechten selecteren; anders werkt Security Manager niet goed.

6. Klik op **Inzenden** om de wijzigingen op te slaan.
7. Start Security Manager opnieuw.

Standaard associaties tussen toegangsrechten en rollen in Security Manager

Deze tabel laat zien hoe de toegangsrechten van Security Manager worden geassocieerd met de rollen van CiscoWorks Gemeenschappelijke services en de standaardrollen in Cisco Secure ACS.

Toestemmingen	Roles							
	Systeembeheer	Security Admin (ACS)	Security Approver (ACS)	Netwerkbeheerder (CW)	Netwerkbeheerder (ACS)	naderen	Netwerkoperator	helpdesk
Toestemmingen bekijken								
Apparaat weergeven	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Beleidsbeleid weergeven	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Objecten bekijken	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Topologie bekijken	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
CLI bekijken	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nee
Admin weergeven	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nee
Archief van Config	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Apparaatbeheer weergeven	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nee
Wachttijden wijzigen								
Apparaat wijzigen	Ja	Ja	Nee	Ja	Nee	Nee	Nee	Nee
Hierarchie	Ja	Ja	Ne	Ja	Ne	Ne	Ne	Nee

wijzigen			e		e	e	e	
Beleid wijzigen	Ja	Ja	Nee	Ja	Nee	Nee	Nee	Nee
Afbeelding wijzigen	Ja	Ja	Nee	Ja	Nee	Nee	Nee	Nee
Objecten wijzigen	Ja	Ja	Nee	Ja	Nee	Nee	Nee	Nee
Topologie wijzigen	Ja	Ja	Nee	Ja	Nee	Nee	Nee	Nee
Admin wijzigen	Ja	Nee	Nee	Nee	Nee	Nee	Nee	Nee
Archief van configuratie wijzigen	Ja	Ja	Nee	Ja	Ja	Nee	Ja	Nee
Aanvullende rechten								
Toewijzings beleid	Ja	Ja	Nee	Ja	Nee	Nee	Nee	Nee
Beleid goedkeuren	Ja	Nee	Ja	Nee	Nee	Nee	Nee	Nee
CLI goedkeuren	Ja	Nee	Nee	Nee	Nee	Ja	Nee	Nee
Opzoeken (importeren)	Ja	Ja	Nee	Ja	Nee	Nee	Nee	Nee
implementeren	Ja	Nee	Nee	Ja	Ja	Nee	Nee	Nee
Beheer	Ja	Nee	Nee	Ja	Ja	Nee	Ja	Nee
Indienen	Ja	Ja	Nee	Ja	Nee	Nee	Nee	Nee

Gerelateerde informatie

- Ondersteuning voor Cisco Security Manager
- Technische ondersteuning en documentatie – Cisco Systems