CSM 3.x: Imposta autorizzazioni e ruoli utente

Sommario

Introduzione

In questo documento viene descritto come configurare le autorizzazioni e i ruoli per gli utenti in Cisco Security Manager (CSM).

Prerequisiti

Requisiti

per le successive spiegazioni, si presume che il CSM sia installato e funzioni correttamente.

Componenti usati

Le informazioni fornite in questo documento si basano sul CSM 3.1.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Imposta autorizzazioni utente

Cisco Security Manager autentica il nome utente e la password prima che l'utente possa accedere. Dopo l'autenticazione, Security Manager stabilisce il ruolo all'interno dell'applicazione. Questo ruolo definisce le autorizzazioni (denominate anche privilegi), ovvero l'insieme di attività o operazioni che l'utente è autorizzato a eseguire. Se non si dispone dell'autorizzazione per determinate operazioni o periferiche, le voci di menu, le voci di sommario e i pulsanti correlati sono nascosti o disattivati. Viene inoltre visualizzato un messaggio che indica che non si dispone dell'autorizzazione per visualizzare le informazioni selezionate o eseguire l'operazione selezionata.

L'autenticazione e l'autorizzazione per Security Manager sono gestite dal server CiscoWorks o da Cisco Secure Access Control Server (ACS). Per impostazione predefinita, CiscoWorks gestisce l'autenticazione e l'autorizzazione, ma è possibile passare a Cisco Secure ACS utilizzando la pagina di configurazione della modalità AAA in CiscoWorks Common Services.

I principali vantaggi dell'uso di Cisco Secure ACS sono la capacità di creare ruoli utente altamente granulari con set di autorizzazioni specializzate (ad esempio, consentendo all'utente di configurare alcuni tipi di criteri ma non altri) e la capacità di limitare gli utenti a determinati dispositivi configurando gruppi di dispositivi di rete (NDG).

Negli argomenti seguenti vengono descritte le autorizzazioni utente:

- Autorizzazioni di Security Manager
- Informazioni sui ruoli CiscoWorks
- Informazioni sui ruoli Cisco Secure ACS
- Associazioni predefinite tra autorizzazioni e ruoli in Security Manager

Autorizzazioni di Security Manager

Security Manager classifica le autorizzazioni nelle categorie come indicato:

1. **Visualizza (View)** - Consente di visualizzare le impostazioni correnti. Per ulteriori informazioni, vedere Visualizzare le autorizzazioni.
2. **Modifica (Modify)** - Consente di modificare le impostazioni correnti. Per ulteriori informazioni, vedere Modifica di autorizzazioni.
3. **Assegna**: consente di assegnare criteri ai dispositivi e alle topologie VPN. Per ulteriori informazioni, vedere Assegnare autorizzazioni
4. **Approva**: consente di approvare le modifiche ai criteri e i processi di distribuzione. Per ulteriori informazioni, vedere Approvare le autorizzazioni.
5. **Importa**: consente di importare in Security Manager le configurazioni già distribuite sui dispositivi.

6. **Distribuisci**: consente di distribuire le modifiche alla configurazione ai dispositivi della rete ed eseguire il rollback per tornare a una configurazione distribuita in precedenza.
7. **Controllo (Control**) - Consente di inviare comandi ai dispositivi, ad esempio ping.
8. **Sottometti (Submit**) - Consente di sottomettere le modifiche alla configurazione per l'approvazione.

- Quando si selezionano le autorizzazioni di modifica, assegnazione, approvazione, importazione, controllo o distribuzione, è necessario selezionare anche le autorizzazioni di visualizzazione corrispondenti. in caso contrario, Security Manager non funzionerà correttamente.
- Quando si seleziona Modifica autorizzazioni criterio, è necessario selezionare anche le autorizzazioni di assegnazione e visualizzazione corrispondenti.
- Quando si autorizza un criterio che utilizza oggetti criterio come parte della relativa definizione, è necessario concedere autorizzazioni di visualizzazione anche a questi tipi di oggetto. Ad esempio, se si seleziona l'autorizzazione per la modifica dei criteri di instradamento, è necessario selezionare anche le autorizzazioni per la visualizzazione degli oggetti di rete e dei ruoli di interfaccia, ovvero i tipi di oggetto richiesti dai criteri di instradamento.
- Lo stesso vale quando si autorizza un oggetto che utilizza altri oggetti come parte della sua definizione. Ad esempio, se si seleziona l'autorizzazione per modificare i gruppi di utenti, è necessario selezionare anche le autorizzazioni per visualizzare gli oggetti di rete, gli oggetti ACL e i gruppi di server AAA.

Visualizza autorizzazioni

Le autorizzazioni di visualizzazione (sola lettura) in Security Manager sono suddivise nelle categorie riportate di seguito.

- Visualizza autorizzazioni criteri
- Visualizza oggetti - Autorizzazioni
- Autorizzazioni visualizzazione aggiuntive

Visualizza autorizzazioni criteri

Security Manager include le autorizzazioni di visualizzazione per i criteri seguenti:

1. **Visualizza > Criteri > Firewall.** Consente di visualizzare i criteri dei servizi firewall (disponibili in Selettore criteri in Firewall) su dispositivi PIX/ASA/FWSM, router IOS e dispositivi Catalyst 6500/7600. Esempi di criteri dei servizi firewall includono regole di accesso, regole AAA e regole di ispezione.
2. **Visualizza > Criteri > Sistema di prevenzione delle intrusioni.** Consente di visualizzare i criteri IPS (presenti nel selettore dei criteri in IPS), inclusi i criteri per IPS in esecuzione sui router IOS.
3. **Visualizza > Criteri > Immagine.** Consente di selezionare un pacchetto di aggiornamento della firma nella procedura guidata Applica aggiornamenti IPS (in Strumenti > Applica aggiornamento IPS), ma non consente di assegnare il pacchetto a dispositivi specifici, a meno che non si disponga anche dell'autorizzazione Elabora > Criteri > Immagine.
4. **Visualizza > Criteri > NAT**. Consente di visualizzare i criteri di conversione degli indirizzi di

rete su dispositivi PIX/ASA/FWSM e router IOS. Esempi di policy NAT includono regole statiche e dinamiche.

5. **Visualizza > Criteri > VPN da sito a sito**. Consente di visualizzare i criteri VPN da sito a sito su dispositivi PIX/ASA/FWSM, router IOS e dispositivi Catalyst 6500/7600. Esempi di criteri VPN da sito a sito includono proposte IKE, proposte IPSec e chiavi già condivise.
6. **Visualizza > Criteri > VPN ad accesso remoto**. Consente di visualizzare i criteri VPN di accesso remoto su dispositivi PIX/ASA/FWSM, router IOS e dispositivi Catalyst 6500/7600. Esempi di criteri VPN per l'accesso remoto includono proposte IKE, proposte IPSec e criteri PKI.
7. **Visualizza > Criteri > VPN SSL**. Consente di visualizzare i criteri VPN SSL su dispositivi PIX/ASA/FWSM e router IOS, ad esempio la procedura guidata VPN SSL.
8. **Visualizza > Criteri > Interfacce**. Consente di visualizzare i criteri di interfaccia (situati nel selettore dei criteri in Interfacce) su dispositivi PIX/ASA/FWSM, router IOS, sensori IPS e dispositivi Catalyst 6500/7600.Su dispositivi PIX/ASA/FWSM, questa autorizzazione copre le porte hardware e le impostazioni dell'interfaccia.Sui router IOS, questa autorizzazione copre le impostazioni di interfaccia di base e avanzate, nonché altri criteri relativi all'interfaccia, come DSL, PVC, PPP e criteri di connessione.Sui sensori IPS, questa autorizzazione copre le interfacce fisiche e le mappe di riepilogo.Sui dispositivi Catalyst 6500/7600, questa autorizzazione copre le interfacce e le impostazioni VLAN.
9. **Visualizza > Criteri > Bridging**. Consente di visualizzare i criteri della tabella ARP (che si trovano in Selezione criteri in Piattaforma > Bridging) sui dispositivi PIX/ASA/FWSM.
10. **Visualizza > Criteri > Amministrazione dispositivi**. Consente di visualizzare i criteri di amministrazione dei dispositivi (situati in Selezione criteri in Piattaforma > Amministrazione dispositivi) sui dispositivi PIX/ASA/FWSM, sui router IOS e sui dispositivi Catalyst 6500/7600:Sui dispositivi PIX/ASA/FWSM, ad esempio, le policy di accesso ai dispositivi, le policy di accesso ai server e le policy di failover.Sui router IOS, esempi includono criteri di accesso ai dispositivi (incluso l'accesso alla linea), criteri di accesso ai server, AAA e Secure Device Provisioning.Nei sensori IPS, questa autorizzazione copre i criteri di accesso ai dispositivi e ai server.Sui dispositivi Catalyst 6500/7600, questa autorizzazione copre le impostazioni IDSM e gli elenchi degli accessi VLAN.
11. **Visualizza > Criteri > Identità**. Consente di visualizzare i criteri di identità (situati in Selezione criteri in Piattaforma > Identità) sui router Cisco IOS, inclusi i criteri 802.1x e NAC (Network Admission Control).
12. **Visualizza > Criteri > Registrazione**. Consente di visualizzare i criteri di registrazione (che si trovano in Selezione criteri in Piattaforma > Registrazione) su dispositivi PIX/ASA/FWSM, router IOS e sensori IPS. Esempi di criteri di registrazione includono l'impostazione della registrazione, la configurazione del server e i criteri del server syslog.
13. **Visualizza > Criteri > Multicast**. Consente di visualizzare i criteri multicast (situati in Selezione criteri in Piattaforma > Multicast) su dispositivi PIX/ASA/FWSM. Esempi di criteri multicast includono routing multicast e criteri IGMP.
14. **Visualizza > Criteri > QoS**. Consente di visualizzare i criteri QoS (situati in Selezione criteri in Piattaforma > Qualità del servizio) sui router Cisco IOS.
15. **Visualizza > Criteri > Instradamento**. Consente di visualizzare i criteri di routing (situati in Selezione criteri in Piattaforma > Routing) sui dispositivi PIX/ASA/FWSM e sui router IOS. Esempi di criteri di routing includono OSPF, RIP e criteri di routing statici.
16. **Visualizza > Criteri > Sicurezza**. Consente di visualizzare i criteri di sicurezza (che si trovano in Selezione criteri in Piattaforma > Sicurezza) su dispositivi PIX/ASA/FWSM e sensori IPS:Sui dispositivi PIX/ASA/FWSM, le policy di sicurezza includono le impostazioni

anti-spoofing, frammentazione e timeout.Sui sensori IPS, i criteri di protezione includono le impostazioni di blocco.

17. **Visualizza > Criteri > Regole criteri servizio**. Consente di visualizzare i criteri delle regole dei criteri di servizio (disponibili in Piattaforma > Regole criteri di servizio nel selettore criteri) sui dispositivi PIX 7.x/ASA. Gli esempi includono le code di priorità e le regole IPS, QoS e di connessione.
18. **Visualizza > Criteri > Preferenze utente**. Consente di visualizzare il criterio di distribuzione (situato in Selezione criteri in Piattaforma > Preferenze utente) sui dispositivi PIX/ASA/FWSM. Questo criterio contiene un'opzione per cancellare tutte le traduzioni NAT durante la distribuzione.
19. **Visualizza > Criteri > Dispositivo virtuale**. Consente di visualizzare i criteri dei sensori virtuali sui dispositivi IPS. Questo criterio viene utilizzato per creare sensori virtuali.
20. **Visualizza > Criteri > FlexConfig**. Consente di visualizzare FlexConfigs, ovvero comandi e istruzioni CLI aggiuntivi che possono essere distribuiti su dispositivi PIX/ASA/FWSM, router IOS e dispositivi Catalyst 6500/7600.

Visualizza oggetti - Autorizzazioni

Security Manager include le autorizzazioni di visualizzazione seguenti per gli oggetti:

1. **Visualizza > Oggetti > Gruppi di server AAA**. Consente di visualizzare gli oggetti del gruppo di server AAA. Questi oggetti vengono utilizzati nei criteri che richiedono i servizi AAA (autenticazione, autorizzazione e accounting).
2. **Visualizza > Oggetti > Server AAA**. Consente di visualizzare gli oggetti server AAA. Questi oggetti rappresentano singoli server AAA definiti come parte di un gruppo di server AAA.
3. **Visualizza > Oggetti > Access Control Lists - Standard/Esteso**. Consente di visualizzare gli oggetti ACL standard ed estesi. Gli oggetti ACL estesi vengono usati per una varietà di policy, ad esempio NAT e NAC, e per stabilire l'accesso VPN. Gli oggetti ACL standard vengono utilizzati per policy come OSPF e SNMP, nonché per stabilire l'accesso VPN.
4. **Visualizza > Oggetti > Access Control Lists** - Web. Consente di visualizzare gli oggetti ACL Web. Gli oggetti ACL Web vengono utilizzati per eseguire il filtro del contenuto nei criteri VPN SSL.
5. **Visualizza > Oggetti > Gruppi di utenti ASA**. Consente di visualizzare gli oggetti del gruppo di utenti ASA. Questi oggetti sono configurati sulle appliance di sicurezza ASA nelle configurazioni Easy VPN, Remote Access VPN e SSL VPN.
6. **Visualizza > Oggetti > Categorie**. Consente di visualizzare gli oggetti categoria. Questi oggetti consentono di identificare facilmente regole e oggetti nelle tabelle delle regole mediante l'utilizzo di colori.
7. **Visualizza > Oggetti > Credenziali**. Consente di visualizzare gli oggetti credenziali. Questi oggetti vengono utilizzati nella configurazione Easy VPN durante l'autenticazione estesa IKE (Xauth).
8. **Visualizza > Oggetti > FlexConfigs**. Consente di visualizzare gli oggetti FlexConfig. Questi oggetti, che contengono comandi di configurazione con istruzioni aggiuntive per il linguaggio di script, possono essere utilizzati per configurare comandi non supportati dall'interfaccia utente di Security Manager.
9. **Visualizza > Oggetti > Proposte IKE**. Consente di visualizzare gli oggetti della proposta IKE. Questi oggetti contengono i parametri necessari per le proposte IKE nei criteri VPN di accesso remoto.

10. **Visualizza > Oggetti > Controlla - Mappe classi** - DNS. Consente di visualizzare gli oggetti mappa classe DNS. Questi oggetti corrispondono al traffico DNS con criteri specifici in modo che sia possibile eseguire azioni su tale traffico.
11. **Visualizza > Oggetti > Ispeziona - Mappe classi - FTP**. Consente di visualizzare gli oggetti mappa della classe FTP. Questi oggetti corrispondono al traffico FTP con criteri specifici in modo che sia possibile eseguire azioni su tale traffico.
12. **Visualizza > Oggetti > Controlla - Mappe classi - HTTP**. Consente di visualizzare gli oggetti mappa classe HTTP. Questi oggetti corrispondono al traffico HTTP con criteri specifici in modo che sia possibile eseguire azioni su tale traffico.
13. **Visualizza > Oggetti > Controlla - Mappe classi - Messaggistica immediata**. Consente di visualizzare gli oggetti mappa della classe IM. Questi oggetti corrispondono al traffico IM con criteri specifici in modo che sia possibile eseguire azioni su tale traffico.
14. **Visualizza > Oggetti > Ispeziona - Mappe classi - SIP**. Consente di visualizzare gli oggetti mappa classe SIP. Questi oggetti associano il traffico SIP a criteri specifici in modo che sia possibile eseguire azioni sul traffico in questione.
15. **Visualizza > Oggetti > Controlla - Mappe criteri - DNS.** Consente di visualizzare gli oggetti mappa dei criteri DNS. Questi oggetti vengono utilizzati per creare mappe di ispezione per il traffico DNS.
16. **Visualizza > Oggetti > Ispeziona - Mappe criteri - FTP.** Consente di visualizzare gli oggetti mappa criteri FTP. Questi oggetti vengono utilizzati per creare mappe di ispezione per il traffico FTP.
17. **Visualizza > Oggetti > Ispeziona - Mappe criteri - GTP**. Consente di visualizzare gli oggetti mappa dei criteri GTP. Questi oggetti vengono usati per creare mappe di ispezione per il traffico GTP.
18. **Visualizza > Oggetti > Ispeziona - Mappe criteri - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Consente di visualizzare gli oggetti mappa dei criteri HTTP creati per i dispositivi ASA/PIX 7.1.x e i router IOS. Questi oggetti vengono utilizzati per creare mappe di ispezione per il traffico HTTP.
19. **Visualizza > Oggetti > Ispeziona - Mappe criteri - HTTP (ASA7.2/PIX7.2)**. Consente di visualizzare gli oggetti mappa dei criteri HTTP creati per i dispositivi ASA 7.2/PIX 7.2. Questi oggetti vengono utilizzati per creare mappe di ispezione per il traffico HTTP.
20. **Visualizza > Oggetti > Ispeziona - Mappe politiche - IM (ASA7.2/PIX7.2)**. Consente di visualizzare gli oggetti mappa dei criteri IM creati per i dispositivi ASA 7.2/PIX 7.2. Questi oggetti vengono utilizzati per creare mappe di ispezione per il traffico IM.
21. **Visualizza > Oggetti > Ispeziona - Mappe criteri - IM (IOS)**. Consente di visualizzare gli oggetti mappa dei criteri IM creati per i dispositivi IOS. Questi oggetti vengono utilizzati per creare mappe di ispezione per il traffico IM.
22. **Visualizza > Oggetti > Ispeziona - Mappe criteri - SIP**. Consente di visualizzare gli oggetti mappa dei criteri SIP. Questi oggetti vengono utilizzati per creare mappe di ispezione per il traffico SIP.
23. **Visualizza > Oggetti > Controlla - Espressioni regolari**. Consente di visualizzare gli oggetti espressione regolare. Questi oggetti rappresentano singole espressioni regolari definite come parte di un gruppo di espressioni regolari.
24. **Visualizza > Oggetti > Controlla - Gruppi di espressioni regolari**. Consente di visualizzare gli oggetti del gruppo di espressioni regolari. Questi oggetti vengono utilizzati da determinate mappe di classe e ispezionano le mappe per verificare la corrispondenza del testo all'interno di un pacchetto.
25. **Visualizza > Oggetti > Controlla - Mappe TCP**. Consente di visualizzare gli oggetti mappa

TCP. Questi oggetti personalizzano l'ispezione sul flusso TCP in entrambe le direzioni.

26. **Visualizza > Oggetti > Ruoli interfaccia**. Consente di visualizzare gli oggetti ruolo interfaccia. Questi oggetti definiscono modelli di denominazione che possono rappresentare più interfacce su diversi tipi di dispositivi. I ruoli interfaccia consentono di applicare criteri a interfacce specifiche su più dispositivi senza dover definire manualmente il nome di ogni interfaccia.
27. **Visualizza > Oggetti > Insiemi trasformazioni IPSec**. Consente di visualizzare gli oggetti set di trasformazioni IPSec. Questi oggetti includono una combinazione di protocolli di sicurezza, algoritmi e altre impostazioni che specificano esattamente la modalità di crittografia e autenticazione dei dati nel tunnel IPsec.
28. **Visualizza > Oggetti > Mappe attributi LDAP**. Consente di visualizzare gli oggetti mappa attributi LDAP. Questi oggetti vengono utilizzati per mappare nomi di attributi personalizzati (definiti dall'utente) ai nomi di attributi LDAP di Cisco.
29. **Visualizza > Oggetti > Reti/Host**. Consente di visualizzare gli oggetti di rete/host. Questi oggetti sono insiemi logici di indirizzi IP che rappresentano reti, host o entrambi. Gli oggetti di rete/host consentono di definire i criteri senza specificare singolarmente ogni rete o host.
30. **Visualizza > Oggetti > Iscrizioni PKI**. Consente di visualizzare gli oggetti di registrazione PKI. Questi oggetti definiscono i server Autorità di certificazione (CA) che operano all'interno di un'infrastruttura a chiave pubblica.
31. **Visualizza > Oggetti > Elenchi inoltro porte**. Consente di visualizzare gli oggetti dell'elenco di inoltro porte. Questi oggetti definiscono i mapping dei numeri di porta in un client remoto all'indirizzo IP dell'applicazione e alla porta dietro un gateway VPN SSL.
32. **Visualizza > Oggetti > Configurazioni desktop sicure**. Consente di visualizzare gli oggetti di configurazione del desktop protetto. Questi oggetti sono componenti denominati riutilizzabili a cui possono fare riferimento i criteri VPN SSL per fornire un mezzo affidabile per eliminare tutte le tracce di dati sensibili condivisi per la durata di una sessione VPN SSL.
33. **Visualizza > Oggetti > Servizi - Elenchi porte**. Consente di visualizzare gli oggetti dell'elenco delle porte. Questi oggetti, che contengono uno o più intervalli di numeri di porta, vengono utilizzati per semplificare il processo di creazione degli oggetti assistenza.
34. **Visualizza > Oggetti > Servizi/Gruppi di servizi** Consente di visualizzare gli oggetti dei servizi e dei gruppi di servizi. Questi oggetti sono mapping definiti di definizioni di porte e protocolli che descrivono i servizi di rete utilizzati dai criteri, ad esempio Kerberos, SSH e POP3.
35. **Visualizza > Oggetti > Server Single Sign-On**. Consente di visualizzare gli oggetti server Single Sign-On. Single Sign-On (SSO) consente agli utenti VPN SSL di immettere un nome utente e una password una volta e di accedere a più servizi protetti e server Web.
36. **Visualizza > Oggetti > Monitor SLA**. Consente di visualizzare gli oggetti di monitoraggio del contratto di servizio. Questi oggetti vengono utilizzati dalle appliance di sicurezza PIX/ASA che eseguono la versione 7.2 o successive per eseguire il tracciamento del percorso. Questa funzionalità consente di tenere traccia della disponibilità di un percorso primario e di installare un percorso di backup in caso di errore del percorso primario.
37. **Visualizza > Oggetti > Personalizzazioni VPN SSL**. Consente di visualizzare gli oggetti di personalizzazione VPN SSL. Questi oggetti definiscono come modificare l'aspetto delle pagine VPN SSL visualizzate agli utenti, ad esempio Login/Logout e Home page.
38. **Visualizza > Oggetti > Gateway VPN SSL**. Consente di visualizzare gli oggetti gateway VPN SSL. Questi oggetti definiscono i parametri che consentono di utilizzare il gateway come proxy per le connessioni alle risorse protette nella VPN SSL.
39. **Visualizza > Oggetti > Oggetti stile**. Consente di visualizzare gli oggetti stile. Questi oggetti

consentono di configurare gli elementi di stile, ad esempio le caratteristiche e i colori dei caratteri, per personalizzare l'aspetto della pagina VPN SSL visualizzata agli utenti VPN SSL quando si connettono all'accessorio di protezione.

40. **Visualizza > Oggetti > Oggetti di testo**. Consente di visualizzare gli oggetti di testo in formato libero. Questi oggetti comprendono una coppia nome-valore, in cui il valore può essere una singola stringa, un elenco di stringhe o una tabella di stringhe.
41. **Visualizza > Oggetti > Intervalli di tempo.** Consente di visualizzare gli oggetti dell'intervallo di tempo. Questi oggetti vengono usati quando si creano ACL con limiti di tempo e regole di ispezione. Vengono anche usati quando si definiscono i gruppi di utenti ASA per limitare l'accesso VPN a orari specifici durante la settimana.
42. **Visualizza > Oggetti > Flussi di traffico**. Consente di visualizzare gli oggetti del flusso del traffico. Questi oggetti definiscono flussi di traffico specifici per l'uso con i dispositivi PIX 7.x/ASA 7.x.
43. **Visualizza > Oggetti > Elenchi URL**. Consente di visualizzare gli oggetti dell'elenco URL. Questi oggetti definiscono gli URL visualizzati nella pagina del portale dopo un accesso riuscito. Ciò consente agli utenti di accedere alle risorse disponibili sui siti Web VPN SSL quando operano in modalità di accesso senza client.
44. **Visualizza > Oggetti > Gruppi di utenti**. Consente di visualizzare gli oggetti del gruppo di utenti. Questi oggetti definiscono i gruppi di client remoti utilizzati nelle topologie Easy VPN, nelle VPN ad accesso remoto e nelle VPN SSL.
45. **Visualizza > Oggetti > Elenchi server WINS**. Consente di visualizzare gli oggetti dell'elenco dei server WINS. Questi oggetti rappresentano i server WINS, utilizzati dalla VPN SSL per accedere o condividere file su sistemi remoti.
46. **Visualizza > Oggetti > Interno - Regole DN**. Consente di visualizzare le regole DN utilizzate dai criteri DN. Si tratta di un oggetto interno utilizzato da Security Manager che non viene visualizzato in Policy Object Manager.
47. **Visualizza > Oggetti > Interno - Aggiornamenti client**. Si tratta di un oggetto interno richiesto dagli oggetti del gruppo di utenti che non viene visualizzato in Gestione oggetti criteri.
48. **Visualizza > Oggetti > Interno - ACE standard**. Si tratta di un oggetto interno per le voci di controllo di accesso standard, utilizzate dagli oggetti ACL.
49. **Visualizza > Oggetti > Interno - ACE estesi.** Si tratta di un oggetto interno per le voci di controllo di accesso estese, utilizzate dagli oggetti ACL.

Autorizzazioni visualizzazione aggiuntive

Security Manager include le seguenti autorizzazioni di visualizzazione aggiuntive:

1. **Visualizza > Amministrazione**. Consente di visualizzare le impostazioni amministrative di Security Manager.
2. **Visualizza > CLI**. Consente di visualizzare i comandi CLI configurati su un dispositivo e di visualizzare in anteprima i comandi che stanno per essere distribuiti.
3. **Visualizza > Config Archive**. Consente di visualizzare l'elenco delle configurazioni contenute nell'archivio di configurazione. Non è possibile visualizzare la configurazione del dispositivo o i comandi CLI.
4. **Visualizza > Dispositivi**. Consente di visualizzare le periferiche in visualizzazione Periferica e tutte le informazioni correlate, incluse le impostazioni delle periferiche, le proprietà, le assegnazioni e così via.
5. **Visualizza > Gestione dispositivi**. Consente di avviare versioni di sola lettura dei device

manager per singoli dispositivi, ad esempio Cisco Router e Security Device Manager (SDM) per router Cisco IOS.
6. **Visualizza > Topologia**. Consente di visualizzare le mappe configurate nella visualizzazione Mappa.

Modifica autorizzazioni

Le autorizzazioni di modifica (lettura/scrittura) in Security Manager sono suddivise nelle categorie riportate di seguito.

- Autorizzazioni modifica criteri
- Autorizzazioni modifica oggetti
- Autorizzazioni di modifica aggiuntive

Autorizzazioni modifica criteri

Nota: quando si specificano i permessi di modifica dei criteri, assicurarsi di aver selezionato anche i permessi di assegnazione e visualizzazione dei criteri corrispondenti.

Security Manager include le autorizzazioni di modifica seguenti per i criteri:

1. **Modifica > Criteri > Firewall**. Consente di modificare i criteri dei servizi firewall (situati in Selettore criteri sotto Firewall) su dispositivi PIX/ASA/FWSM, router IOS e dispositivi Catalyst 6500/7600. Esempi di criteri dei servizi firewall includono regole di accesso, regole AAA e regole di ispezione.
2. **Elabora > Criteri > Sistema di prevenzione delle intrusioni**. Consente di modificare i criteri IPS (presenti nel selettore dei criteri in IPS), inclusi i criteri per IPS in esecuzione sui router IOS. Questa autorizzazione consente inoltre di ottimizzare le firme nell'Aggiornamento guidato firme, disponibile in Strumenti > Applica aggiornamento IPS.
3. **Elabora > Criteri > Immagine**. Consente di assegnare un pacchetto di aggiornamento della firma ai dispositivi nella procedura guidata Applica aggiornamenti IPS (in Strumenti > Applica aggiornamento IPS). Questa autorizzazione consente inoltre di assegnare le impostazioni di aggiornamento automatico a dispositivi specifici (disponibili in Strumenti > Amministrazione Security Manager > Aggiornamenti IPS).
4. **Modifica > Criteri > NAT**. Consente di modificare le policy di conversione degli indirizzi di rete su dispositivi PIX/ASA/FWSM e router IOS. Esempi di policy NAT includono regole statiche e dinamiche.
5. **Modifica > Criteri > VPN da sito a sito**. Consente di modificare i criteri VPN da sito a sito su dispositivi PIX/ASA/FWSM, router IOS e dispositivi Catalyst 6500/7600. Esempi di criteri VPN da sito a sito includono proposte IKE, proposte IPSec e chiavi già condivise.
6. **Modifica > Criteri > VPN ad accesso remoto**. Consente di modificare i criteri VPN di accesso remoto su dispositivi PIX/ASA/FWSM, router IOS e dispositivi Catalyst 6500/7600. Esempi di criteri VPN per l'accesso remoto includono proposte IKE, proposte IPSec e criteri PKI.
7. **Modifica > Criteri > VPN SSL**. Consente di modificare i criteri VPN SSL su dispositivi PIX/ASA/FWSM e router IOS, ad esempio la procedura guidata VPN SSL.
8. **Modifica > Criteri > Interfacce**. Consente di modificare i criteri di interfaccia (disponibili nel selettore criteri in Interfacce) su dispositivi PIX/ASA/FWSM, router IOS, sensori IPS e dispositivi Catalyst 6500/7600:Su dispositivi PIX/ASA/FWSM, questa autorizzazione copre le

porte hardware e le impostazioni dell'interfaccia.Sui router IOS, questa autorizzazione copre le impostazioni di interfaccia di base e avanzate, nonché altri criteri relativi all'interfaccia, come DSL, PVC, PPP e criteri di connessione.Sui sensori IPS, questa autorizzazione copre le interfacce fisiche e le mappe di riepilogo.Sui dispositivi Catalyst 6500/7600, questa autorizzazione copre le interfacce e le impostazioni VLAN.

9. **Modifica > Criteri > Bridging**. Consente di modificare i criteri della tabella ARP (che si trovano in Selezione criteri in Piattaforma > Bridging) sui dispositivi PIX/ASA/FWSM.
10. **Modifica > Criteri > Amministrazione dispositivi**. Consente di modificare i criteri di amministrazione dei dispositivi (situati in Selezione criteri in Piattaforma > Amministrazione dispositivi) su dispositivi PIX/ASA/FWSM, router IOS e dispositivi Catalyst 6500/7600:Sui dispositivi PIX/ASA/FWSM, ad esempio, le policy di accesso ai dispositivi, le policy di accesso ai server e le policy di failover.Sui router IOS, esempi includono criteri di accesso ai dispositivi (incluso l'accesso alla linea), criteri di accesso ai server, AAA e Secure Device Provisioning.Nei sensori IPS, questa autorizzazione copre i criteri di accesso ai dispositivi e ai server.Sui dispositivi Catalyst 6500/7600, questa autorizzazione copre le impostazioni IDSM e l'elenco degli accessi VLAN.
11. **Modifica > Criteri > Identità**. Consente di modificare i criteri di identità (situati in Selezione criteri in Piattaforma > Identità) sui router Cisco IOS, inclusi i criteri 802.1x e NAC (Network Admission Control).
12. **Modifica > Criteri > Registrazione**. Consente di modificare i criteri di registrazione (situati in Selezione criteri in Piattaforma > Registrazione) su dispositivi PIX/ASA/FWSM, router IOS e sensori IPS. Esempi di criteri di registrazione includono l'impostazione della registrazione, la configurazione del server e i criteri del server syslog.
13. **Modifica > Criteri > Multicast**. Consente di modificare i criteri multicast (situati in Selezione criteri in Piattaforma > Multicast) su dispositivi PIX/ASA/FWSM. Esempi di criteri multicast includono routing multicast e criteri IGMP.
14. **Modifica > Criteri > QoS**. Consente di modificare i criteri QoS (presenti nel selettore criteri in Piattaforma > Qualità del servizio) sui router Cisco IOS.
15. **Modifica > Criteri > Instradamento**. Consente di modificare i criteri di routing (situati in Selezione criteri in Piattaforma > Routing) su dispositivi PIX/ASA/FWSM e router IOS. Esempi di criteri di routing includono OSPF, RIP e criteri di routing statici.
16. **Modifica > Criteri > Protezione**. Consente di modificare i criteri di sicurezza (situati in Selezione criteri in Piattaforma > Sicurezza) su dispositivi PIX/ASA/FWSM e sensori IPS:Sui dispositivi PIX/ASA/FWSM, le policy di sicurezza includono le impostazioni anti-spoofing, frammentazione e timeout.Sui sensori IPS, i criteri di protezione includono le impostazioni di blocco.
17. **Modifica > Criteri > Regole criteri servizio**. Consente di modificare i criteri delle regole dei criteri di servizio (disponibili in Piattaforma > Regole criteri di servizio nel selettore criteri) sui dispositivi PIX 7.x/ASA. Gli esempi includono le code di priorità e le regole IPS, QoS e di connessione.
18. **Modifica > Criteri > Preferenze utente**. Consente di modificare il criterio di distribuzione (posizionato in Selezione criteri in Piattaforma > Preferenze utente) sui dispositivi PIX/ASA/FWSM. Questo criterio contiene un'opzione per cancellare tutte le traduzioni NAT durante la distribuzione.
19. **Modifica > Criteri > Dispositivo virtuale**. Consente di modificare i criteri dei sensori virtuali sui dispositivi IPS. Utilizzare questo criterio per creare sensori virtuali.
20. **Modifica > Criteri > FlexConfig**. Consente di modificare FlexConfigs, ovvero comandi e istruzioni CLI aggiuntivi che possono essere distribuiti su dispositivi PIX/ASA/FWSM, router

IOS e dispositivi Catalyst 6500/7600.

Autorizzazioni modifica oggetti

Security Manager include le autorizzazioni di visualizzazione seguenti per gli oggetti:

1. **Modifica > Oggetti > Gruppi di server AAA**. Consente di visualizzare gli oggetti del gruppo di server AAA. Questi oggetti vengono utilizzati nei criteri che richiedono i servizi AAA (autenticazione, autorizzazione e accounting).
2. **Elabora > Oggetti > Server AAA**. Consente di visualizzare gli oggetti server AAA. Questi oggetti rappresentano singoli server AAA definiti come parte di un gruppo di server AAA.
3. **Modifica > Oggetti > Access Control Lists - Standard/Esteso**. Consente di visualizzare gli oggetti ACL standard ed estesi. Gli oggetti ACL estesi vengono usati per una varietà di policy, ad esempio NAT e NAC, e per stabilire l'accesso VPN. Gli oggetti ACL standard vengono utilizzati per policy come OSPF e SNMP, nonché per stabilire l'accesso VPN.
4. **Modifica > Oggetti > Access Control Lists - Web**. Consente di visualizzare gli oggetti ACL Web. Gli oggetti ACL Web vengono utilizzati per eseguire il filtro del contenuto nei criteri VPN SSL.
5. **Modifica > Oggetti >** Gruppi di utenti **ASA**. Consente di visualizzare gli oggetti del gruppo di utenti ASA. Questi oggetti sono configurati sulle appliance di sicurezza ASA nelle configurazioni Easy VPN, Remote Access VPN e SSL VPN.
6. **Modifica > Oggetti > Categorie**. Consente di visualizzare gli oggetti categoria. Questi oggetti consentono di identificare facilmente regole e oggetti nelle tabelle delle regole mediante l'utilizzo di colori.
7. **Modifica > Oggetti > Credenziali**. Consente di visualizzare gli oggetti credenziali. Questi oggetti vengono utilizzati nella configurazione Easy VPN durante l'autenticazione estesa IKE (Xauth).
8. **Modifica > Oggetti > FlexConfigs**. Consente di visualizzare gli oggetti FlexConfig. Questi oggetti, che contengono comandi di configurazione con istruzioni aggiuntive per il linguaggio di script, possono essere utilizzati per configurare comandi non supportati dall'interfaccia utente di Security Manager.
9. **Modifica > Oggetti > Proposte IKE**. Consente di visualizzare gli oggetti della proposta IKE. Questi oggetti contengono i parametri necessari per le proposte IKE nei criteri VPN di accesso remoto.
10. **Elabora > Oggetti > Controlla - Mappe classi - DNS**. Consente di visualizzare gli oggetti mappa classe DNS. Questi oggetti corrispondono al traffico DNS con criteri specifici in modo che sia possibile eseguire azioni su tale traffico.
11. **Modifica > Oggetti > Controlla - Mappe classi - FTP**. Consente di visualizzare gli oggetti mappa della classe FTP. Questi oggetti corrispondono al traffico FTP con criteri specifici in modo che sia possibile eseguire azioni su tale traffico.
12. **Modifica > Oggetti > Controlla - Mappe classi - HTTP**. Consente di visualizzare gli oggetti mappa classe HTTP. Questi oggetti corrispondono al traffico HTTP con criteri specifici in modo che sia possibile eseguire azioni su tale traffico.
13. **Modifica > Oggetti > Ispeziona - Mappe classi - Messaggistica immediata**. Consente di visualizzare gli oggetti mappa della classe IM. Questi oggetti corrispondono al traffico IM con criteri specifici in modo che sia possibile eseguire azioni su tale traffico.
14. **Elabora > Oggetti > Ispeziona - Mappe classi - SIP**. Consente di visualizzare gli oggetti mappa classe SIP. Questi oggetti associano il traffico SIP a criteri specifici in modo che sia

possibile eseguire azioni sul traffico in questione.

15. **Elabora > Oggetti > Controlla - Mappe criteri - DNS**. Consente di visualizzare gli oggetti mappa dei criteri DNS. Questi oggetti vengono utilizzati per creare mappe di ispezione per il traffico DNS.
16. **Elabora > Oggetti > Ispeziona - Mappe criteri - FTP**. Consente di visualizzare gli oggetti mappa criteri FTP. Questi oggetti vengono utilizzati per creare mappe di ispezione per il traffico FTP.
17. **Elabora > Oggetti > Ispeziona - Mappe criteri - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Consente di visualizzare gli oggetti mappa dei criteri HTTP creati per i dispositivi ASA/PIX 7.x e i router IOS. Questi oggetti vengono utilizzati per creare mappe di ispezione per il traffico HTTP.
18. **Elabora > Oggetti > Ispeziona - Mappe criteri - HTTP (ASA7.2/PIX7.2)**. Consente di visualizzare gli oggetti mappa dei criteri HTTP creati per i dispositivi ASA 7.2/PIX 7.2. Questi oggetti vengono utilizzati per creare mappe di ispezione per il traffico HTTP.
19. **Elabora > Oggetti > Ispeziona - Mappe criteri - Messaggistica immediata (ASA7.2/PIX7.2)**. Consente di visualizzare gli oggetti mappa dei criteri IM creati per i dispositivi ASA 7.2/PIX 7.2. Questi oggetti vengono utilizzati per creare mappe di ispezione per il traffico IM.
20. **Elabora > Oggetti > Ispeziona - Mappe criteri - IM (IOS)**. Consente di visualizzare gli oggetti mappa dei criteri IM creati per i dispositivi IOS. Questi oggetti vengono utilizzati per creare mappe di ispezione per il traffico IM.
21. **Elabora > Oggetti > Ispeziona - Mappe criteri - SIP**. Consente di visualizzare gli oggetti mappa dei criteri SIP. Questi oggetti vengono utilizzati per creare mappe di ispezione per il traffico SIP.
22. **Elabora > Oggetti > Controlla - Espressioni regolari**. Consente di visualizzare gli oggetti espressione regolare. Questi oggetti rappresentano singole espressioni regolari definite come parte di un gruppo di espressioni regolari.
23. **Modifica > Oggetti > Controlla - Gruppi di espressioni regolari**. Consente di visualizzare gli oggetti del gruppo di espressioni regolari. Questi oggetti vengono utilizzati da determinate mappe di classe e ispezionano le mappe per verificare la corrispondenza del testo all'interno di un pacchetto.
24. **Elabora > Oggetti > Controlla - Mappe TCP**. Consente di visualizzare gli oggetti mappa TCP. Questi oggetti personalizzano l'ispezione sul flusso TCP in entrambe le direzioni.
25. **Modifica > Oggetti > Ruoli interfaccia**. Consente di visualizzare gli oggetti ruolo interfaccia. Questi oggetti definiscono modelli di denominazione che possono rappresentare più interfacce su diversi tipi di dispositivi. I ruoli interfaccia consentono di applicare criteri a interfacce specifiche su più dispositivi senza dover definire manualmente il nome di ogni interfaccia.
26. **Elabora > Oggetti > Insiemi trasformazioni IPSec**. Consente di visualizzare gli oggetti set di trasformazioni IPSec. Questi oggetti includono una combinazione di protocolli di sicurezza, algoritmi e altre impostazioni che specificano esattamente la modalità di crittografia e autenticazione dei dati nel tunnel IPsec.
27. **Modifica > Oggetti > Mappe attributi LDAP**. Consente di visualizzare gli oggetti mappa attributi LDAP. Questi oggetti vengono utilizzati per mappare nomi di attributi personalizzati (definiti dall'utente) ai nomi di attributi LDAP di Cisco.
28. **Elabora > Oggetti > Reti/Host**. Consente di visualizzare gli oggetti di rete/host. Questi oggetti sono insiemi logici di indirizzi IP che rappresentano reti, host o entrambi. Gli oggetti di rete/host consentono di definire i criteri senza specificare singolarmente ogni rete o host.
29. **Modifica > Oggetti > Iscrizioni PKI**. Consente di visualizzare gli oggetti di registrazione PKI. Questi oggetti definiscono i server Autorità di certificazione (CA) che operano all'interno di

un'infrastruttura a chiave pubblica.

30. **Elabora > Oggetti > Elenchi inoltro porte**. Consente di visualizzare gli oggetti dell'elenco di inoltro porte. Questi oggetti definiscono i mapping dei numeri di porta in un client remoto all'indirizzo IP dell'applicazione e alla porta dietro un gateway VPN SSL.
31. **Elabora > Oggetti > Configurazioni desktop sicure**. Consente di visualizzare gli oggetti di configurazione del desktop protetto. Questi oggetti sono componenti denominati riutilizzabili a cui possono fare riferimento i criteri VPN SSL per fornire un mezzo affidabile per eliminare tutte le tracce di dati sensibili condivisi per la durata di una sessione VPN SSL.
32. **Modifica > Oggetti > Servizi - Elenchi porte**. Consente di visualizzare gli oggetti dell'elenco delle porte. Questi oggetti, che contengono uno o più intervalli di numeri di porta, vengono utilizzati per semplificare il processo di creazione degli oggetti assistenza.
33. **Elabora > Oggetti > Servizi/Gruppi di servizi.** Consente di visualizzare gli oggetti servizio e gruppo di servizi. Questi oggetti sono mapping definiti di definizioni di porte e protocolli che descrivono i servizi di rete utilizzati dai criteri, ad esempio Kerberos, SSH e POP3.
34. **Modifica > Oggetti > Server Single Sign-On.** Consente di visualizzare gli oggetti server Single Sign-On. Single Sign-On (SSO) consente agli utenti VPN SSL di immettere un nome utente e una password una volta e di accedere a più servizi protetti e server Web.
35. **Modifica > Oggetti > Monitor SLA**. Consente di visualizzare gli oggetti di monitoraggio del contratto di servizio. Questi oggetti vengono utilizzati dalle appliance di sicurezza PIX/ASA che eseguono la versione 7.2 o successive per eseguire il tracciamento del percorso. Questa funzionalità consente di tenere traccia della disponibilità di un percorso primario e di installare un percorso di backup in caso di errore del percorso primario.
36. **Modifica > Oggetti > Personalizzazioni VPN SSL**. Consente di visualizzare gli oggetti di personalizzazione VPN SSL. Questi oggetti definiscono come modificare l'aspetto delle pagine VPN SSL visualizzate agli utenti, ad esempio Login/Logout e Home page.
37. **Modifica > Oggetti > Gateway VPN SSL**. Consente di visualizzare gli oggetti gateway VPN SSL. Questi oggetti definiscono i parametri che consentono di utilizzare il gateway come proxy per le connessioni alle risorse protette nella VPN SSL.
38. **Elabora > Oggetti > Oggetti stile**. Consente di visualizzare gli oggetti stile. Questi oggetti consentono di configurare gli elementi di stile, ad esempio le caratteristiche e i colori dei caratteri, per personalizzare l'aspetto della pagina VPN SSL visualizzata agli utenti VPN SSL quando si connettono all'accessorio di protezione.
39. **Elabora > Oggetti > Oggetti di testo**. Consente di visualizzare gli oggetti di testo in formato libero. Questi oggetti comprendono una coppia nome-valore, in cui il valore può essere una singola stringa, un elenco di stringhe o una tabella di stringhe.
40. **Modifica > Oggetti > Intervalli di tempo.** Consente di visualizzare gli oggetti dell'intervallo di tempo. Questi oggetti vengono usati quando si creano ACL con limiti di tempo e regole di ispezione. Vengono anche usati quando si definiscono i gruppi di utenti ASA per limitare l'accesso VPN a orari specifici durante la settimana.
41. **Elabora > Oggetti > Flussi di traffico**. Consente di visualizzare gli oggetti del flusso del traffico. Questi oggetti definiscono flussi di traffico specifici per l'uso con i dispositivi PIX 7.x/ASA 7.x.
42. **Modifica > Oggetti > Elenchi URL**. Consente di visualizzare gli oggetti dell'elenco URL. Questi oggetti definiscono gli URL visualizzati nella pagina del portale dopo un accesso riuscito. Ciò consente agli utenti di accedere alle risorse disponibili sui siti Web VPN SSL quando operano in modalità di accesso senza client.
43. **Modifica > Oggetti > Gruppi di utenti**. Consente di visualizzare gli oggetti del gruppo di utenti. Questi oggetti definiscono i gruppi di client remoti utilizzati nelle topologie Easy VPN,

nelle VPN ad accesso remoto e nelle VPN SSL
44. **Modifica > Oggetti > Elenchi server WINS**. Consente di visualizzare gli oggetti dell'elenco dei server WINS. Questi oggetti rappresentano i server WINS, utilizzati dalla VPN SSL per accedere o condividere file su sistemi remoti.
45. **Modifica > Oggetti > Interno - Regole DN.** Consente di visualizzare le regole DN utilizzate dai criteri DN. Si tratta di un oggetto interno utilizzato da Security Manager che non viene visualizzato in Policy Object Manager.
46. **Modifica > Oggetti > Interno - Aggiornamenti client**. Si tratta di un oggetto interno richiesto dagli oggetti del gruppo di utenti che non viene visualizzato in Gestione oggetti criteri.
47. **Modifica > Oggetti > Interno - ACE standard**. Si tratta di un oggetto interno per le voci di controllo di accesso standard, utilizzate dagli oggetti ACL.
48. **Elabora > Oggetti > Interno - ACE esteso**. Si tratta di un oggetto interno per le voci di controllo di accesso estese, utilizzate dagli oggetti ACL.

Autorizzazioni di modifica aggiuntive

Security Manager include le autorizzazioni di modifica aggiuntive come illustrato di seguito:

1. **Elabora > Amministrazione**. Consente di modificare le impostazioni amministrative di Security Manager.
2. **Modifica > Configura archivio**. Consente di modificare la configurazione del dispositivo nell'archivio di configurazione. Consente inoltre di aggiungere configurazioni all'archivio e di personalizzare lo strumento Archivio di configurazione.
3. **Modifica > Dispositivi**. Consente di aggiungere ed eliminare dispositivi, nonché di modificare le proprietà e gli attributi dei dispositivi. Per individuare i criteri nel dispositivo da aggiungere, è necessario abilitare anche l'autorizzazione di importazione. Inoltre, se si abilita l'autorizzazione Modifica > Dispositivi, assicurarsi di abilitare anche l'autorizzazione Assegna > Criteri > Interfacce.
4. **Modifica > Gerarchia**. Consente di modificare i gruppi di dispositivi.
5. **Modifica > Topologia**. Consente di modificare le mappe nella visualizzazione Mappa.

Assegna autorizzazioni

Security Manager include le autorizzazioni per l'assegnazione dei criteri come illustrato di seguito:

1. **Assegna > Criteri > Firewall**. Consente di assegnare i criteri dei servizi firewall (situati in Selettore criteri sotto Firewall) ai dispositivi PIX/ASA/FWSM, ai router IOS e ai dispositivi Catalyst 6500/7600. Esempi di criteri dei servizi firewall includono regole di accesso, regole AAA e regole di ispezione.
2. **Assegnare > Criteri > Sistema di prevenzione delle intrusioni**. Consente di assegnare i criteri IPS (disponibili in Selezione criteri in IPS), inclusi i criteri per IPS in esecuzione sui router IOS.
3. **Assegna > Criteri > Immagine**. Questa autorizzazione non è attualmente utilizzata da Security Manager.
4. **Assegna > Criteri > NAT**. Consente di assegnare i criteri di conversione degli indirizzi di rete ai dispositivi PIX/ASA/FWSM e ai router IOS. Esempi di policy NAT includono regole statiche e dinamiche.
5. **Assegna > Criteri > VPN da sito a sito**. Consente di assegnare criteri VPN da sito a sito a

dispositivi PIX/ASA/FWSM, router IOS e dispositivi Catalyst 6500/7600. Esempi di criteri VPN da sito a sito includono proposte IKE, proposte IPSec e chiavi già condivise.

6. **Assegna > Criteri > VPN ad accesso remoto**. Consente di assegnare criteri VPN di accesso remoto a dispositivi PIX/ASA/FWSM, router IOS e dispositivi Catalyst 6500/7600. Esempi di criteri VPN per l'accesso remoto includono proposte IKE, proposte IPSec e criteri PKI.
7. **Assegna > Criteri > VPN SSL**. Consente di assegnare i criteri VPN SSL ai dispositivi PIX/ASA/FWSM e ai router IOS, ad esempio la procedura guidata VPN SSL.
8. **Assegna > Criteri > Interfacce**. Consente di assegnare i criteri di interfaccia (situati in Policy selector sotto Interfaces) ai dispositivi PIX/ASA/FWSM, ai router IOS e ai dispositivi Catalyst 6500/7600:Su dispositivi PIX/ASA/FWSM, questa autorizzazione copre le porte hardware e le impostazioni dell'interfaccia.Sui router IOS, questa autorizzazione copre le impostazioni di interfaccia di base e avanzate, nonché altri criteri relativi all'interfaccia, come DSL, PVC, PPP e criteri di connessione.Sui dispositivi Catalyst 6500/7600, questa autorizzazione copre le interfacce e le impostazioni VLAN.
9. **Assegna > Criteri > Bridging**. Consente di assegnare i criteri della tabella ARP (che si trova in Selezione criterio in Piattaforma > Bridging) ai dispositivi PIX/ASA/FWSM.
10. **Assegna > Criteri > Amministrazione dispositivi**. Consente di assegnare i criteri di amministrazione dei dispositivi (situati in Selezione criteri in Piattaforma > Amministrazione dispositivi) ai dispositivi PIX/ASA/FWSM, ai router IOS e ai dispositivi Catalyst 6500/7600:Sui dispositivi PIX/ASA/FWSM, ad esempio, le policy di accesso ai dispositivi, le policy di accesso ai server e le policy di failover.Sui router IOS, esempi includono criteri di accesso ai dispositivi (incluso l'accesso alla linea), criteri di accesso ai server, AAA e Secure Device Provisioning.Nei sensori IPS, questa autorizzazione copre i criteri di accesso ai dispositivi e ai server.Sui dispositivi Catalyst 6500/7600, questa autorizzazione copre le impostazioni IDSM e gli elenchi degli accessi VLAN.
11. **Assegna > Criteri > Identità**. Consente di assegnare i criteri di identità (situati in Selezione criteri in Piattaforma > Identità) ai router Cisco IOS, inclusi i criteri 802.1x e NAC (Network Admission Control).
12. **Assegna > Criteri > Registrazione**. Consente di assegnare i criteri di registrazione (situati in Selezione criteri in Piattaforma > Registrazione) ai dispositivi PIX/ASA/FWSM e ai router IOS. Esempi di criteri di registrazione includono l'impostazione della registrazione, la configurazione del server e i criteri del server syslog.
13. **Assegna > Criteri > Multicast**. Consente di assegnare i criteri multicast (situati in Selezione criteri in Piattaforma > Multicast) ai dispositivi PIX/ASA/FWSM. Esempi di criteri multicast includono routing multicast e criteri IGMP.
14. **Assegnare > Criteri > QoS**. Consente di assegnare i criteri QoS (situati in Selezione criteri in Piattaforma > Qualità del servizio) ai router Cisco IOS.
15. **Assegna > Criteri > Instradamento**. Consente di assegnare le policy di routing (posizionate nel selettore Policy in Piattaforma > Routing) ai dispositivi PIX/ASA/FWSM e ai router IOS. Esempi di criteri di routing includono OSPF, RIP e criteri di routing statici.
16. **Assegna > Criteri > Sicurezza**. Consente di assegnare i criteri di sicurezza (situati in Selezione criteri in Piattaforma > Sicurezza) ai dispositivi PIX/ASA/FWSM. I criteri di sicurezza includono le impostazioni di protezione dallo spoofing, dai frammenti e dal timeout.
17. **Assegna > Criteri > Regole criteri servizio**. Consente di assegnare ai dispositivi PIX 7.x/ASA i criteri delle regole dei criteri di servizio (disponibili nel selettore Criteri in Piattaforma > Regole criteri di servizio). Gli esempi includono le code di priorità e le regole IPS, QoS e di connessione.

18. **Assegna > Criteri > Preferenze utente**. Consente di assegnare il criterio di distribuzione (situato in Selezione criteri in Piattaforma > Preferenze utente) ai dispositivi PIX/ASA/FWSM. Questo criterio contiene un'opzione per cancellare tutte le traduzioni NAT durante la distribuzione.
19. **Assegna > Criteri > Dispositivo virtuale**. Consente di assegnare criteri dei sensori virtuali ai dispositivi IPS. Utilizzare questo criterio per creare sensori virtuali.
20. **Assegna > Criteri > FlexConfig**. Consente di assegnare FlexConfigs, ovvero comandi e istruzioni CLI aggiuntivi che possono essere distribuiti a dispositivi PIX/ASA/FWSM, router IOS e dispositivi Catalyst 6500/7600.

Nota: quando si specificano le autorizzazioni di assegnazione, assicurarsi di aver selezionato anche le autorizzazioni di visualizzazione corrispondenti.

Approva autorizzazioni

Security Manager fornisce le autorizzazioni di approvazione come illustrato di seguito:

1. **Approvare > CLI**. Consente di approvare le modifiche ai comandi CLI contenute in un processo di distribuzione.
2. **Approva > Politica**. Consente di approvare le modifiche alla configurazione contenute nei criteri configurati in un'attività del flusso di lavoro.

Informazioni sui ruoli CiscoWorks

Agli utenti creati in CiscoWorks Common Services vengono assegnati uno o più ruoli. Le autorizzazioni associate a ogni ruolo determinano le operazioni che ogni utente è autorizzato a eseguire in Security Manager.

Negli argomenti seguenti vengono descritti i ruoli di CiscoWorks:

- Ruoli predefiniti dei servizi comuni di CiscoWorks
- Assegnazione di ruoli agli utenti in CiscoWorks Common Services

Ruoli predefiniti dei servizi comuni di CiscoWorks

CiscoWorks Common Services contiene i ruoli predefiniti seguenti:

1. **Help Desk**: gli utenti dell'help desk possono visualizzare (ma non modificare) dispositivi, policy, oggetti e mappe topologiche.
2. **Operatore di rete**: oltre a visualizzare le autorizzazioni, gli operatori di rete possono visualizzare i comandi CLI e le impostazioni amministrative di Security Manager. Gli operatori di rete possono anche modificare l'archivio di configurazione e inviare comandi (ad esempio, ping) ai dispositivi.
3. **Approvatore**: oltre alle autorizzazioni di visualizzazione, gli approvatori possono approvare o rifiutare i processi di distribuzione. Non possono eseguire la distribuzione.
4. **Amministratore di rete**: gli amministratori di rete dispongono di autorizzazioni complete di visualizzazione e modifica, ad eccezione della modifica delle impostazioni amministrative. Possono rilevare i dispositivi e i criteri configurati su tali dispositivi, assegnare i criteri ai dispositivi e inviare comandi ai dispositivi. Gli amministratori di rete non possono approvare

attività o processi di distribuzione. tuttavia, possono distribuire processi approvati da altri.
5. **Amministratore di sistema**: gli amministratori di sistema hanno accesso completo a tutte le autorizzazioni di Security Manager, inclusi la modifica, l'assegnazione di criteri, l'approvazione di attività e processi, il rilevamento, la distribuzione e l'invio di comandi ai dispositivi.

Nota: se nel server sono installate applicazioni aggiuntive, è possibile che in Servizi comuni vengano visualizzati ruoli aggiuntivi, ad esempio i dati di esportazione. Il ruolo Esporta dati è destinato a sviluppatori di terze parti e non viene utilizzato da Security Manager.

Suggerimento: Sebbene non sia possibile modificare la definizione dei ruoli CiscoWorks, è possibile definire i ruoli assegnati a ogni utente. Per ulteriori informazioni, vedere Assegnazione di ruoli agli utenti nei servizi comuni CiscoWorks.

Assegnazione di ruoli agli utenti in CiscoWorks Common Services

CiscoWorks Common Services consente di definire i ruoli assegnati a ogni utente. Modificando la definizione del ruolo di un utente, si modificano i tipi di operazioni che l'utente è autorizzato a eseguire in Security Manager. Ad esempio, se si assegna il ruolo Help Desk, l'utente è limitato alle operazioni di visualizzazione e non può modificare alcun dato. Tuttavia, se si assegna il ruolo Operatore di rete, l'utente può anche modificare l'archivio di configurazione. È possibile assegnare più ruoli a ogni utente.

Nota: è necessario riavviare Security Manager dopo aver apportato modifiche alle autorizzazioni utente.

Procedura:

1. In Servizi comuni selezionare **Server > Protezione**, quindi **Gestione trust server singolo > Configurazione utente locale** dal sommario.**Suggerimento:** per accedere alla pagina Impostazione utente locale da Security Manager, selezionare Strumenti > Amministrazione Security Manager > Protezione server, quindi fare clic su Impostazione utente locale.
2. Selezionare la casella di controllo accanto a un utente esistente, quindi fare clic su **Modifica**.
3. Nella pagina Informazioni utente selezionare i ruoli da assegnare all'utente facendo clic sulle caselle di controllo.Per ulteriori informazioni su ogni ruolo, vedere Ruoli predefiniti dei servizi comuni di CiscoWorks.
4. Fare clic su **OK** per salvare le modifiche.
5. Riavviare Security Manager.

Informazioni sui ruoli Cisco Secure ACS

Cisco Secure ACS offre una maggiore flessibilità per la gestione delle autorizzazioni di Security Manager rispetto a CiscoWorks, in quanto supporta ruoli specifici dell'applicazione che è possibile configurare. Ogni ruolo è costituito da un insieme di autorizzazioni che determinano il livello di autorizzazione per le attività di Security Manager. In Cisco Secure ACS, si assegna un ruolo a ogni gruppo di utenti (e, facoltativamente, anche ai singoli utenti), consentendo a ogni utente di tale gruppo di eseguire le operazioni autorizzate dalle autorizzazioni definite per quel ruolo.

Inoltre, è possibile assegnare questi ruoli ai gruppi di dispositivi Cisco Secure ACS, consentendo di differenziare le autorizzazioni su set di dispositivi diversi.

Nota: i gruppi di dispositivi Cisco Secure ACS sono indipendenti dai gruppi di dispositivi di Security Manager.

Negli argomenti seguenti vengono descritti i ruoli di Cisco Secure ACS:

- Ruoli predefiniti Cisco Secure ACS
- Personalizzazione dei ruoli Cisco Secure ACS

Ruoli predefiniti Cisco Secure ACS

Cisco Secure ACS include gli stessi ruoli di CiscoWorks (vedere Informazioni sui ruoli di CiscoWorks), oltre ai seguenti ruoli aggiuntivi:

1. **Security Approver**: gli approvatori della sicurezza possono visualizzare (ma non modificare) dispositivi, policy, oggetti, mappe, comandi CLI e impostazioni amministrative. Gli approvatori della sicurezza possono inoltre approvare o rifiutare le modifiche alla configurazione contenute in un'attività. Non possono approvare o rifiutare il processo di distribuzione, né eseguire la distribuzione.
2. **Amministratore della sicurezza**: oltre a disporre delle autorizzazioni di visualizzazione, gli amministratori della sicurezza possono modificare dispositivi, gruppi di dispositivi, policy, oggetti e mappe topologiche. Possono inoltre assegnare policy a dispositivi e topologie VPN ed eseguire il rilevamento per importare nuovi dispositivi nel sistema.
3. **Amministratore di rete**: oltre alle autorizzazioni di visualizzazione, gli amministratori di rete possono modificare l'archivio di configurazione, eseguire la distribuzione ed eseguire comandi sui dispositivi.

Nota: le autorizzazioni contenute nel ruolo di amministratore di rete Cisco Secure ACS sono diverse da quelle contenute nel ruolo di amministratore di rete CiscoWorks. Per ulteriori informazioni, vedere Informazioni sui ruoli CiscoWorks.

A differenza di CiscoWorks, Cisco Secure ACS consente di personalizzare le autorizzazioni associate a ogni ruolo di Security Manager. Per ulteriori informazioni sulla modifica dei ruoli predefiniti, vedere Personalizzazione dei ruoli Cisco Secure ACS.

Nota: per ottenere l'autorizzazione di Security Manager, è necessario installare Cisco Secure ACS 3.3 o versione successiva.

Personalizzazione dei ruoli Cisco Secure ACS

Cisco Secure ACS consente di modificare le autorizzazioni associate a ciascun ruolo di Security Manager. È inoltre possibile personalizzare Cisco Secure ACS creando ruoli utente specializzati con autorizzazioni destinate a particolari attività di Security Manager.

Nota: è necessario riavviare Security Manager dopo aver apportato modifiche alle autorizzazioni utente.

Procedura:

1. In Cisco Secure ACS, fare clic su **Shared Profile Components** (Componenti profilo condiviso) sulla barra di navigazione.
2. Fare clic su **Cisco Security Manager** nella pagina Componenti condivisi. Vengono visualizzati

i ruoli configurati per Security Manager.

3. Effettuare una delle seguenti operazioni:Per creare un ruolo, fare clic su **Aggiungi**. Andare al Passaggio 4.Per modificare un ruolo esistente, fare clic sul ruolo. Andare al Passaggio 5.
4. Immettere un nome per il ruolo e, facoltativamente, una descrizione.
5. Selezionare e deselezionare le caselle di controllo nella struttura delle autorizzazioni per definire le autorizzazioni per questo ruoloSe si seleziona la casella di controllo relativa a un ramo della struttura verranno selezionate tutte le autorizzazioni del ramo. Ad esempio, selezionando **Assegna** vengono selezionate tutte le autorizzazioni di assegnazione.Per un elenco completo delle autorizzazioni di Security Manager, vedere Autorizzazioni di Security Manager.**Nota:** quando si seleziona Modifica, approva, assegna, importa, controlla o distribuisci autorizzazioni, è necessario selezionare anche le autorizzazioni di visualizzazione corrispondenti. in caso contrario, Security Manager non funzionerà correttamente.
6. Fare clic su **Invia** per salvare le modifiche.
7. Riavviare Security Manager.

Associazioni predefinite tra autorizzazioni e ruoli in Security Manager

Nella tabella viene mostrata l'associazione delle autorizzazioni di Security Manager ai ruoli di CiscoWorks Common Services e ai ruoli predefiniti in Cisco Secure ACS.

Autorizzazioni	Ruoli							
	Amministratore di sistema	Security Admin (ACS)	Security Approver (ACS)	Amministratore di rete (CW)	Amministratore di rete (ACS)	Approvatore	Operatore di rete	Helpdesk
Visualizza autorizzazioni								
Visualizza dispositivo	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Visualizza criterio	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Visualizza oggetti	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Visualizza topologia	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Visualizza CLI	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No
Visualizza amministratore	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No

Visualizza archivio di configurazione	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Visualizza gestori dispositivi	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No
Modifica autorizzazioni								
Modifica dispositivo	Sì	Sì	No	Sì	No	No	No	No
Modifica gerarchia	Sì	Sì	No	Sì	No	No	No	No
Modifica criterio	Sì	Sì	No	Sì	No	No	No	No
Modifica immagine	Sì	Sì	No	Sì	No	No	No	No
Modifica oggetti	Sì	Sì	No	Sì	No	No	No	No
Modifica topologia	Sì	Sì	No	Sì	No	No	No	No
Modifica amministratore	Sì	No	No	No	No	No	No	No
Modifica archivio di configurazione	Sì	Sì	No	Sì	Sì	No	Sì	No
Autorizzazioni aggiuntive								
Assegna criterio	Sì	Sì	No	Sì	No	No	No	No
Approva criterio	Sì	No	Sì	No	No	No	No	No
Approva CLI	Sì	No	No	No	No	Sì	No	No
Individua (Importa)	Sì	Sì	No	Sì	No	No	No	No
Implementazione	Sì	No	No	Sì	Sì	No	No	No
Controllo	Sì	No	No	Sì	Sì	No	Sì	No
Invia	Sì	Sì	No	Sì	No	No	No	No

Informazioni correlate

- Pagina di supporto di Cisco Security Manager
- Documentazione e supporto tecnico – Cisco Systems