Cisco IOS op rol gebaseerde toegangscontrole met dm: Configuratietoestemming tussen operationele groepen scheiden

Inhoud

Inleiding

Routing- en beveiligingsfuncties worden traditioneel ondersteund in afzonderlijke apparaten, wat een duidelijke verdeling van de beheerverantwoordelijkheid tussen de netwerkinfrastructuur en de beveiligingsservices biedt. De convergentie van security en routingfunctionaliteit in de Cisco geïntegreerde services routers biedt deze duidelijke scheiding met meerdere apparaten niet aan. Sommige organisaties hebben een segregatie van configuratievermogen nodig om klanten of dienstenbeheergroepen langs functionele grenzen te beperken. CLI Views, een Cisco IOS® Software optie, probeert deze behoefte aan te pakken met Rol-Based CLI Access. Dit document beschrijft de configuratie die door de steun die van Cisco IOS Rol-Based Access Control wordt gedefinieerd wordt, en biedt achtergrondinformatie in de mogelijkheden van CLI Kijken van de Cisco IOS Opdracht-Lijn Interface.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

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 de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Vele organisaties delegeren verantwoordelijkheid voor het onderhoud van routing en infrastructurele connectiviteit aan een groep van netwerkoperaties, en verantwoordelijkheid voor het onderhoud van firewall, VPN, en inbraakpreventiefunctionaliteit aan een groep van veiligheidsoperaties. CLI Views kan de configuratie van de veiligheidsfunctionaliteit en de controlecapaciteit tot de secops groep beperken, en omgekeerd de netwerkconnectiviteit, routing, en andere infrastructurele taken tot de groep van netwerken beperken.

Sommige serviceproviders willen beperkte configuratie- of bewakingsfuncties aan klanten aanbieden, maar willen geen klanten toestaan om andere apparaten instellingen te configureren of bekijken. Opnieuw biedt CLI-views granulaire controle over CLI-mogelijkheid om gebruikers of gebruikersgroepen te beperken tot het uitvoeren van alleen geautoriseerde opdrachten.

Cisco IOS-software heeft een mogelijkheid geboden om CLI-opdrachten met een TACACS+ server te beperken voor goedkeuring om CLI-opdrachten op basis van gebruikersnaam of lidmaatschap van gebruikersgroepen uit te voeren of te weigeren. CLI Views biedt een vergelijkbaar vermogen aan, maar de beleidscontrole wordt toegepast door het lokale apparaat nadat de gespecificeerde weergave van de gebruiker van de AAA server is ontvangen. Wanneer AAA-opdrachtautorisatie wordt gebruikt, moet elke opdracht afzonderlijk zijn geautoriseerd door de AAA-server, wat een regelmatige dialoog tussen het apparaat en de AAA-server veroorzaakt. CLI Views (CLI) staat CLI-beleidscontrole per apparaat toe, terwijl AAA-commandoautorisatie hetzelfde commando machtigingsbeleid toepast op alle apparaten waarop een gebruiker toegang heeft.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Associatie van gebruikers met een visie

De gebruikers kunnen worden geassocieerd met een lokale CLI Beeld door een terugkeereigenschap van AAA of in de lokale configuratie van Verificatie. Voor de lokale configuratie wordt de gebruikersnaam ingesteld met een extra weergaveoptie, die overeenkomt met de geconfigureerde **parser View** name. Deze voorbeeldgebruikers worden ingesteld voor de standaard-dm-beelden:

```
username fw-user privilege [privilege-level] view SDM_Firewall
username monitor-user privilege [privilege-level] view SDM_Monitor
username vpn-user privilege [privilege-level] view SDM_EasyVPN_Remote
username sdm-root privilege [privilege-level] view root
```

Gebruikers die toegewezen zijn aan een bepaalde weergave kunnen tijdelijk naar een andere weergave switches als ze het wachtwoord hebben voor de weergave die ze willen invoeren. Geef deze exec-opdracht af om de standpunten te wijzigen:

```
enable view view-name
```

Configuratie Parser-weergave

CLI View kan van de router CLI, of door middel van een dm worden gevormd. Het middel biedt statische steun voor vier meningen, zoals besproken in het gedeelte van de Ondersteuning van het CLI van het Videoscherm. Om CLI te configureren vanuit de Opdracht-Lijn interface moet een gebruiker worden gedefinieerd als een root-weergavegebruiker, of moet de gebruiker behoren tot de weergave met toegang tot de **parser-**configuratie. De gebruikers die niet met een weergave zijn geassocieerd en die proberen de meningen te configureren krijgen dit bericht:

```
router(config#parser view test-view
No view Active! Switch to View Context
```

CLI-inzichten maken het mogelijk om volledige opdrachthiërarchieën in te sluiten of uit te sluiten voor zowel de uitvoerende als de configuratie-modus, of alleen delen daarvan. Er zijn drie opties beschikbaar om een opdracht of commando hiërarchie in een bepaalde weergave toe te staan of af te wijzen:

```
router(config-view)#commands configure ?
  exclude            Exclude the command from the view
  include            Add command to the view
  include-exclusive  Include in this view but exclude from others
```

CLI View inkorten de in werking stellen-configuratie zodat de configuratie van de Parser Beeld niet wordt weergegeven. Nochtans, is de configuratie van de Beeld van Parser zichtbaar in het opstartende-configuratie.

Raadpleeg Rol-gebaseerde CLI-toegang voor meer informatie over de definitie van weergave.

Associatie Parser View

De gebruikers die aan een Beeld van de Parser worden toegewezen kunnen bepalen aan welke

die mening wordt toegewezen wanneer zij aan een router worden ingelogd. Als het bevel van de **show parser View** voor de gebruikersmeningen toegestaan is, kunnen zij het bevel van de **show parser** bekijken uitgeven om hun mening te bepalen:

```
router#sh parser view
Current view is 'SDM_Firewall'
```

Ondersteuning van SLI-displays

Standaard zal dm drie standaardinstellingen bieden, twee voor configuratie en controle van Firewall en VPN componenten, en één beperkte controle-only weergave. Een extra standaard **root** weergave is ook beschikbaar in DSM.

Het is niet mogelijk om de opdrachten aan te passen die in of uitgesloten zijn van elke standaardinstelling en biedt geen mogelijkheid om extra weergaven te definiëren. Als de extra meningen van het CLI worden bepaald, biedt het CLI-venster niet de extra meningen aan in het configuratiescherm **Gebruikersaccounts/video's**.

Deze meningen en respectieve commando permissies zijn vooraf bepaald voor slechts dm:

ViewBdm_Firewall

```
parser view SDM_Firewall
 secret 5 $1$w/cD$T1ryjKM8aGCnIaKSm.Cx9/
 commands interface include all ip inspect
 commands interface include all ip verify
 commands interface include all ip access-group
 commands interface include ip
 commands interface include description
 commands interface include all no ip inspect
 commands interface include all no ip verify
 commands interface include all no ip access-group
 commands interface include no ip
 commands interface include no description
 commands interface include no
 commands configure include end
 commands configure include all access-list
 commands configure include all ip access-list
 commands configure include all interface
 commands configure include all zone-pair
 commands configure include all zone
 commands configure include all policy-map
 commands configure include all class-map
 commands configure include all parameter-map
 commands configure include all appfw
 commands configure include all ip urlfilter
 commands configure include all ip inspect
 commands configure include all ip port-map
 commands configure include ip cef
 commands configure include ip
 commands configure include all crypto
 commands configure include no end
 commands configure include all no access-list
 commands configure include all no ip access-list
 commands configure include all no interface
 commands configure include all no zone-pair
 commands configure include all no zone
```

```
 commands configure include all no policy-map
 commands configure include all no class-map
 commands configure include all no parameter-map
 commands configure include all no appfw
 commands configure include all no ip urlfilter
 commands configure include all no ip inspect
 commands configure include all no ip port-map
 commands configure include no ip cef
 commands configure include no ip
 commands configure include all no crypto
 commands configure include no
 commands exec include all vlan
 commands exec include dir all-filesystems
 commands exec include dir
 commands exec include crypto ipsec client ezvpn connect
 commands exec include crypto ipsec client ezvpn xauth
 commands exec include crypto ipsec client ezvpn
 commands exec include crypto ipsec client
 commands exec include crypto ipsec
 commands exec include crypto
 commands exec include write memory
 commands exec include write
 commands exec include all ping ip
 commands exec include ping
 commands exec include configure terminal
 commands exec include configure
 commands exec include all show
 commands exec include all debug appfw
 commands exec include all debug ip inspect
 commands exec include debug ip
 commands exec include debug
 commands exec include all clear
```

sm_EasyVPN_Remote-weergave

```
parser view SDM_EasyVPN_Remote
 secret 5 $1$UnC3$ienYd0L7Q/9xfCNkBQ4Uu.
 commands interface include all crypto
 commands interface include all no crypto
 commands interface include no
 commands configure include end
 commands configure include all access-list
 commands configure include ip radius source-interface
 commands configure include ip radius
 commands configure include all ip nat
 commands configure include ip dns server
 commands configure include ip dns
 commands configure include all interface
 commands configure include all dot1x
 commands configure include all identity policy
 commands configure include identity profile
 commands configure include identity
 commands configure include all ip domain lookup
 commands configure include ip domain
 commands configure include ip
 commands configure include all crypto
 commands configure include all aaa
 commands configure include default end
 commands configure include all default access-list
 commands configure include default ip radius source-interface
 commands configure include default ip radius
 commands configure include all default ip nat
 commands configure include default ip dns server
```

```
 commands configure include default ip dns
 commands configure include all default interface
 commands configure include all default dot1x
 commands configure include all default identity policy
 commands configure include default identity profile
 commands configure include default identity
 commands configure include all default ip domain lookup
 commands configure include default ip domain
 commands configure include default ip
 commands configure include all default crypto
 commands configure include all default aaa
 commands configure include default
 commands configure include no end
 commands configure include all no access-list
 commands configure include no ip radius source-interface
 commands configure include no ip radius
 commands configure include all no ip nat
 commands configure include no ip dns server
 commands configure include no ip dns
 commands configure include all no interface
 commands configure include all no dot1x
 commands configure include all no identity policy
 commands configure include no identity profile
 commands configure include no identity
 commands configure include all no ip domain lookup
 commands configure include no ip domain
 commands configure include no ip
 commands configure include all no crypto
 commands configure include all no aaa
 commands configure include no
 commands exec include dir all-filesystems
 commands exec include dir
 commands exec include crypto ipsec client ezvpn connect
 commands exec include crypto ipsec client ezvpn xauth
 commands exec include crypto ipsec client ezvpn
 commands exec include crypto ipsec client
 commands exec include crypto ipsec
 commands exec include crypto
 commands exec include write memory
 commands exec include write
 commands exec include all ping ip
 commands exec include ping
 commands exec include configure terminal
 commands exec include configure
 commands exec include all show
 commands exec include no
 commands exec include all debug appfw
 commands exec include all debug ip inspect
 commands exec include debug ip
 commands exec include debug
 commands exec include all clear
```

dm_monitor-weergave

```
parser view SDM_Monitor
 secret 5 $1$RDYW$OABbxSgtx1kOozLlkBeJ9/
 commands configure include end
 commands configure include all interface
 commands configure include no end
 commands configure include all no interface
 commands exec include dir all-filesystems
 commands exec include dir
 commands exec include all crypto ipsec client ezvpn
```

```
commands exec include crypto ipsec client
commands exec include crypto ipsec
commands exec include crypto
commands exec include all ping ip
commands exec include ping
commands exec include configure terminal
commands exec include configure
commands exec include all show
commands exec include all debug appfw
commands exec include all debug ip inspect
commands exec include debug ip
commands exec include debug
commands exec include all clear
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Op rol gebaseerde CLI-toegang
- Technische ondersteuning en documentatie – Cisco Systems