Uitleggen van de client-id voor bestandsanalyse voor gateway, cloudgateway en e-mail- en webbeheer

Inhoud

Inleiding
Client ID voor bestandsanalyse voor gateway, cloudgateway en e-mail- en webbeheer
Gateway voor cloudgateway
E-mail- en webbeheer
Applicatiegroepering voor rapportage van bestandanalyse
Groepsapplicaties
Gateway voor cloudgateway
E-mail- en webbeheer
Applicaties bekijken
Gateway voor cloudgateway
E-mail- en webbeheer
Aanvullende informatie
Cisco Secure E-mail gateway-documentatie
Documentatie voor beveiligde e-mail met Cloud Gateway
Cisco Secure Email en Web Manager-documentatie
Cisco Secure Malware-analyses
Cisco beveiligde productdocumentatie

Inleiding

Dit document beschrijft hoe u de client-ID voor bestandanalyse kunt vinden voor Cisco Secure Email Gateway, Cloud Gateway en Email and Web Manager. De client-ID voor bestandsanalyse is een unieke registratiesleutel van 65 tekens die wordt gebruikt wanneer de Gateway, Cloud Gateway of Email and Web Manager zich registreert bij Cisco Malware Analytics (voorheen Threat Grid) voor het indienen en sandboxen van bestanden. Als u bijvoorbeeld de service Bestandsanalyse hebt ingeschakeld en de reputatieservice geen informatie heeft over de bestandsbijlage die in een bericht is gevonden, en de bestandsbijlage voldoet aan de criteria voor bestanden die kunnen worden geanalyseerd (zie Ondersteunde bestanden voor bestandsreputatie- en analyseservices), kan het bericht in quarantaine worden geplaatst (zieBerichten in quarantaine plaatsen met bijlagen die voor analyse worden verzonden), en kan het bestand voor analyse worden verzonden.

Bij "Applicatie Groepering voor Rapportage van Bestandsanalyse" dient u er zeker van te zijn dat u uw Bestandsanalyse-ID(en) kent.

Raadpleeg het hoofdstuk "Bestandsreputatie filtering en bestandsanalyse" van de gebruikershandleiding voor volledige informatie:

- Cisco Secure Email Gateway-eindgebruikershandleidingen

- Cisco Secure Email Cloud Gateway-eindgebruikershandleidingen

Client ID voor bestandsanalyse voor gateway, cloudgateway en e-mail- en webbeheer

De client-ID voor bestandsanalyse wordt automatisch gegenereerd voor toestellen wanneer u File Analysis inschakelt.

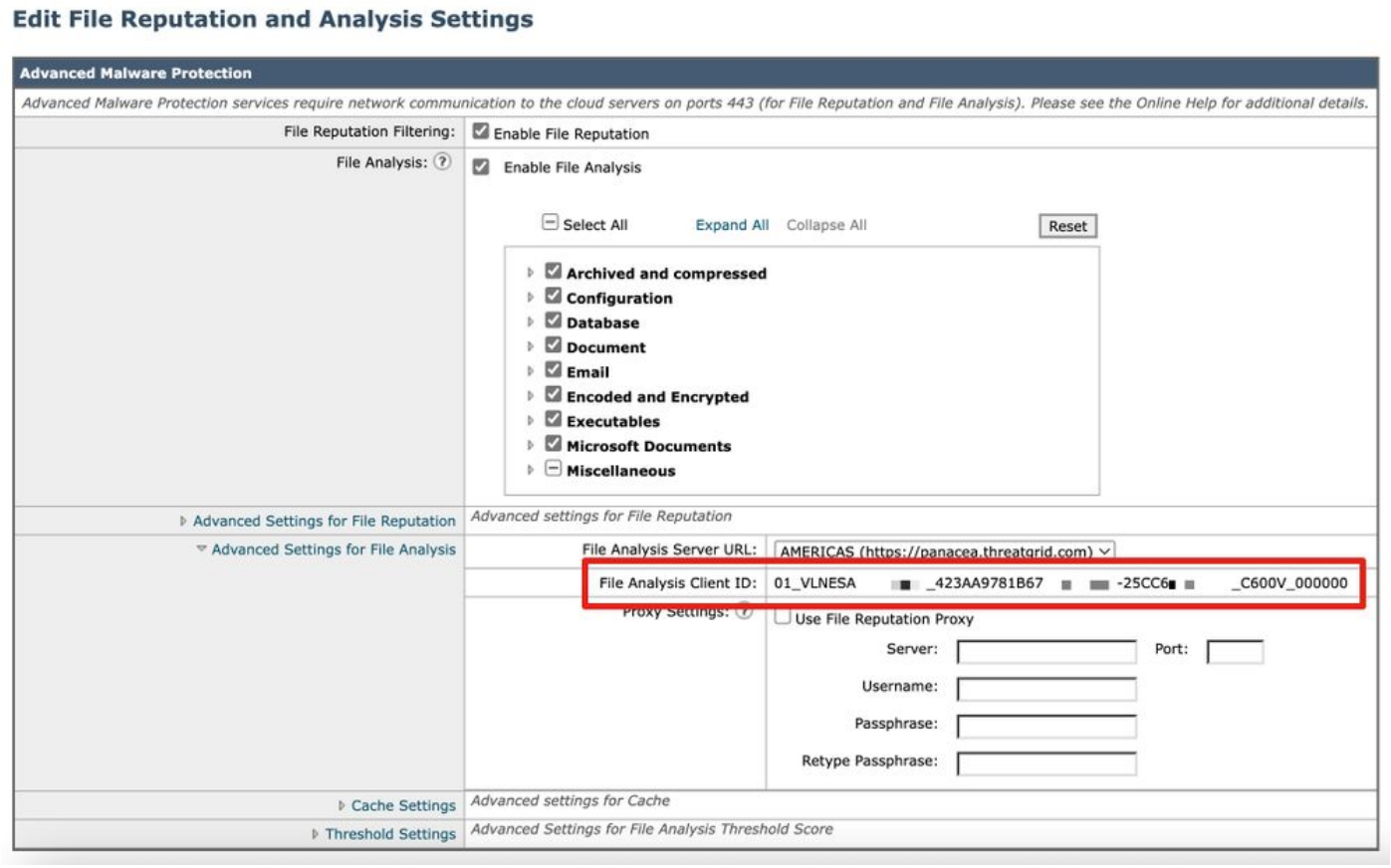
Zorg ervoor dat u over de benodigde functietoetsen en de bestandsreputatie en bestandsanalyse beschikt voordat u begint met de Gateway of Cloud Gateway. Om de functietoetsen te zien, navigeer u naar **Systeembeheer > Functietoetsen**. Bestandsreputatie en bestandsanalyse worden afzonderlijk vermeld en hebben de actieve status.

Gateway voor cloudgateway

1. Log in op de gebruikersinterface.
2. Ga naar **Security Services > Bestandsreputatie en -analyse**.
3. Klik op **Wereldwijde instellingen bewerken...**
4. Breid **geavanceerde instellingen voor bestandanalyse uit**.

De client-ID voor bestandanalyse wordt hier vermeld.

EVoorbeeld:



Opmerking: Er is een verschil in de File Analysis Client ID voor virtuele apparaten versus hardware-apparaten.

De client-id voor bestandsanalyse voor de gateway of cloudgateway is gebaseerd op een tekenreeksindeling van 65 tekens:

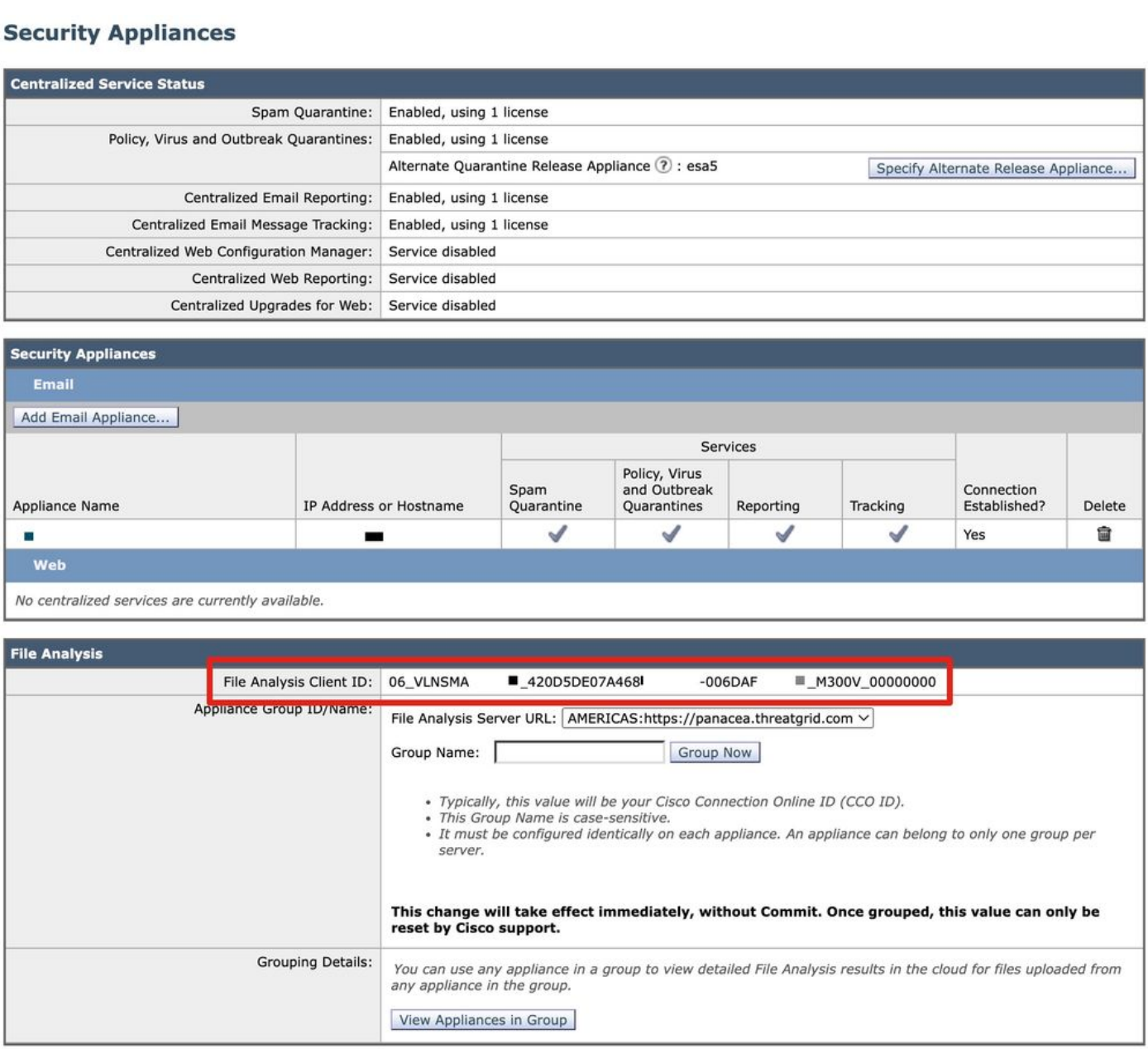
Waarde	Uitleg
01_	"01" is specifiek voor de gateway of cloudgateway.
VLNESAXXXYYY_	Als dit een virtueel apparaat is, gebruikt het de VLN-licentie # (gevonden bij de CLI-opdrachtshowlicentie). Als dit een hardware-apparaat is, is er geen veld.
SERIEEL_	VOLLEDIG serienummer van het apparaat.
CX200V_	Model van het apparaat.
00000000	Veldnullen. Gebaseerd op de vorige velden, variëren deze om het veld van 65 tekens ronden.

E-mail- en webbeheer

1. Log in op de gebruikersinterface.
2. Ga naar **Gecentraliseerd beheer > Security applicatie**.

Onderaan deze pagina staat de sectie Bestandsanalyse. De client-ID voor bestandanalyse wordt hier vermeld.

Voorbeeld:



Opmerking: Er is een verschil in de File Analysis Client ID voor virtuele apparaten versus hardware-apparaten.

De client-id voor bestandsanalyse voor e-mail en webbeheer is gebaseerd op een tekenreeksindeling van 65 tekens:

Waarde	Uitleg
06_	"06" is specifiek voor de Email en Web Manager.
VLNSMAXXXYY_	Als dit een virtueel apparaat is, gebruikt het de VLN-licentie # (gevonden bij de CLI-opdrachtshowlicentie). Als dit een hardware-apparaat is, is er geen veld.
SERIEEL_	VOLLEDIG serienummer van het apparaat.
MX200V_	Model van het apparaat.
000000	Veldnullen. Gebaseerd op de vorige velden, variëren deze om het veld van 65 tekens a ronden.

Applicatiegroepering voor rapportage van bestandanalyse

Als uw licentie toegang tot Cisco Secure Malware Analytics (https://panacea.threatgrid.com) omvat, is het de beste praktijk voor uw Gateway of Cloud Gateway om deze aan uw individuele organisatieaccount te koppelen. Om alle content security applicaties in uw organisatie in staat te stellen om gedetailleerde resultaten in de cloud weer te geven over bestanden die voor analyse worden verzonden vanaf elke Gateway of Cloud Gateway in uw organisatie, moet u alle applicaties bij dezelfde apparaatgroep aansluiten. Wanneer u zich aanmeldt bij Malware Analytics, worden uw inzendingen en bedreigingsmonsters die naar de cloud worden gestuurd voor analyse allemaal weergegeven in het Malware Analytics-dashboard voor uw organisatie.

Opmerking: Cloudgateway-klanten hebben dit ingesteld tijdens activeringen en implementaties die door Cisco worden uitgevoerd.

Groepsapplicaties

Opmerking: Als u een Cloud Gateway hebt en dit is niet voltooid, opent u een ondersteuningscase voordat u een applicatie-groep-id/naam configureert.

Gateway voor cloudgateway

1. Ga vanuit de gebruikersinterface naar **Security Services > File Reputation and Analysis**.
2. Klik op **Klik hier om applicaties te groeperen of weer te geven voor File Analysis rapportage**.
3. Voer uw **apparaatgroep-id/naam in**. De standaardwaarden zijn: Aanbevolen wordt om uw CCOID voor deze waarde te gebruiken.Een apparaat kan tot slechts één groep behoren.Nadat u de functie Bestandsanalyse hebt geconfigureerd, kunt u een machine aan een groep toevoegen.
4. Klik **nu op Groep**.

E-mail- en webbeheer

Opmerking: De optie voor het configureren van een Applicatie Groep ID/Naam is alleen

beschikbaar nadat de E-mail en Web Manager een E-mail applicatie heeft toegevoegd voor gecentraliseerde beheerdoeleinden en het Beleid, Virus, Uitbraak Quarantines heeft gemigreerd.

1. Ga vanuit de gebruikersinterface naar **Gecentraliseerde services > Security applicaties**. Voer uw **apparaatgroep-id/naam in**. De standaardwaarden zijn:Meestal is deze waarde uw Cisco Connection Online ID (CCO-id).Deze groepsnaam is hoofdlettergevoelig.Het moet op elk apparaat identiek worden geconfigureerd. Een apparaat kan tot slechts één groep per server behoren.
2. Klik **nu op Groep**.

Let op:

- Wanneer u een groep-ID toevoegt, wordt het onmiddellijk van kracht, zonder een commit. Als u een groep-ID moet wijzigen, moet u contact opnemen met Cisco TAC.
- Deze naam is hoofdlettergevoelig en moet op elk apparaat in de analysegroep identiek worden geconfigureerd.

Applicaties bekijken

Gateway voor cloudgateway

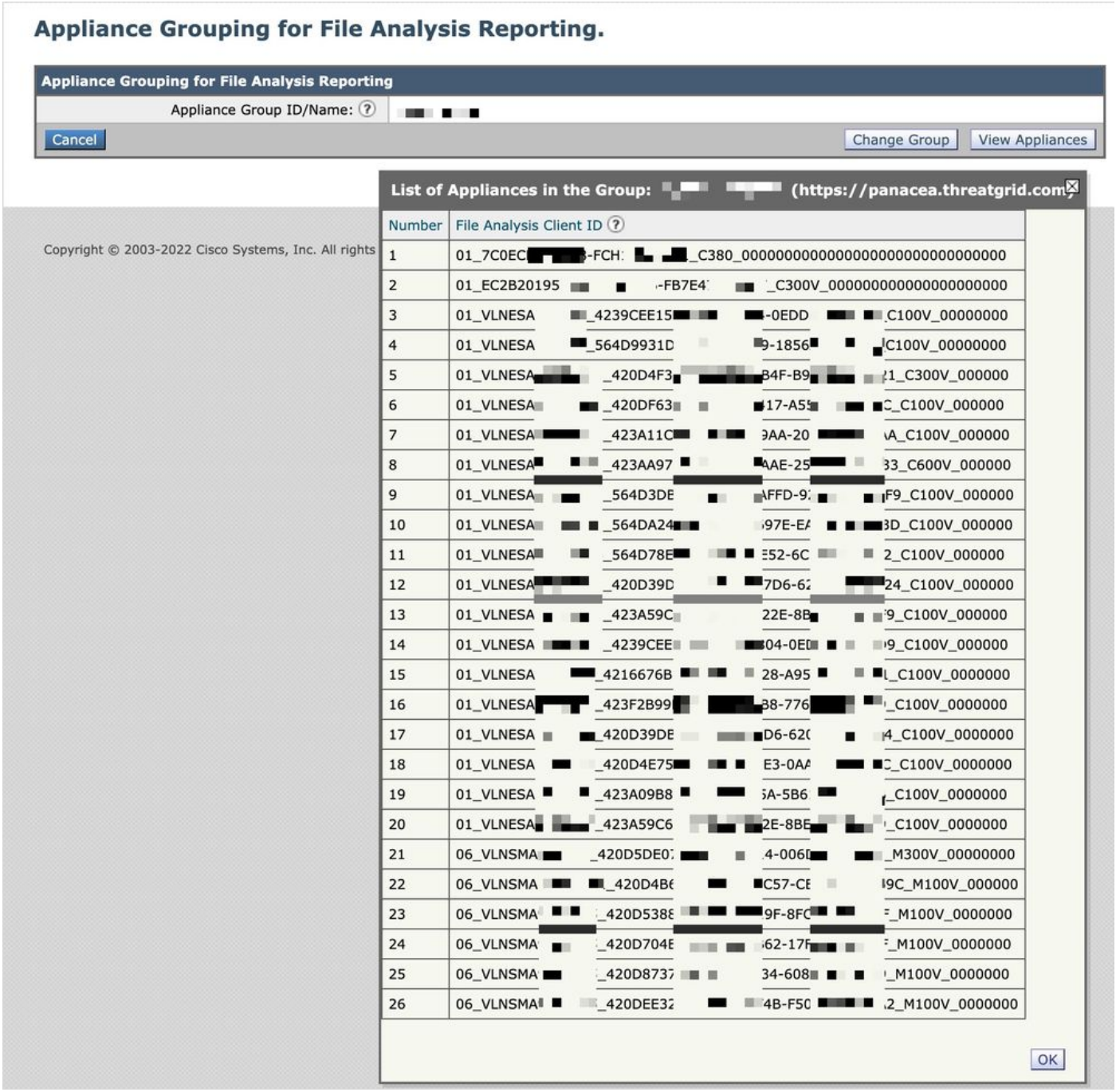
1. Navigeer vanuit de gebruikersinterface naar **Security Services > File Reputation and Analysis.**
2. Klik op **Klik hier om applicaties te groeperen of weer te geven voor File Analysis rapportage**.
3. Klik op **Applicaties bekijken**.

E-mail- en webbeheer

1. Ga vanuit de gebruikersinterface naar **Gecentraliseerde services > Security applicaties**.
2. Klik op **Toepassingen in groep bekijken** in het gedeelte Bestandsanalyse.

De client-ID voor bestandsanalyse van alle apparaten die bij de applicatiegroep-id/naam zijn aangesloten, wordt hier vermeld.

Voorbeeld:



Aanvullende informatie

Cisco Secure E-mail gateway-documentatie

- Release-opmerkingen
- Gebruikershandleiding
- CLI-referentiegids
- API-programmeerhandleidingen voor Cisco Secure Email Gateway
- Open bron die in Cisco Secure Email Gateway wordt gebruikt
- Installatiehandleiding voor Cisco Content Security virtuele applicatie (inclusief vESA)

Documentatie voor beveiligde e-mail met Cloud Gateway

- Release-opmerkingen
- Gebruikershandleiding

Cisco Secure Email en Web Manager-documentatie

- Releaseopmerkingen en compatibiliteitsmatrix
- Gebruikershandleiding
- API-programmeerhandleidingen voor Cisco Secure Email and Web Manager
- Installatiehandleiding voor Cisco Content Security virtuele applicatie (inclusief vSMA)

Cisco Secure Malware-analyses

- Cisco Secure Malware Analytics (Threat Grid)

Cisco beveiligde productdocumentatie

- Cisco Secure-portfolio-naamgevingsarchitectuur

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.