

Hoe maak ik toegangsbeleidsgroepen die overeenkomen met Active Directory-groepen?

Inhoud

[Vraag](#)

Vraag

Hoe maak ik toegangsbeleidsgroepen die overeenkomen met Active Directory (AD)-groepen?

De eerste stap is het configureren van een verificatieleer (NT LAN Manager (NTLM)) en een Identity die het verificatieleer gebruikt.

-
1. Maak een NTLM-domein aan op de Web Security Appliance (WSA) onder Network > Verification.
 2. Zodra u uw NTLM-domein hebt geconfigureerd, kies Web Security Manager > Identiteiten, klik dan op Identiteit toevoegen.
 3. Volg deze stappen om een identiteit te creëren:
 1. Naam: Auth.id
 2. Boven invoegen: 1
 3. Leden door verificatie definiëren: <NTLM-naam domein>
 4. Regeling: Gebruik Basis of NTLMSSP of gebruik NTLMSSP
 5. Alle andere instellingen blijven standaard ingeschakeld.
Als u verificatie wilt testen tegen geselecteerde clients, gebruikt u Leden definiëren op subnet en specificeert u het IP van de verzoekende client. Dit staat WSA toe om authenticatie voor deze geselecteerde slechts cliënten te verzoeken.
 6. Klik op Verzenden.

Op dit punt moet u slechts twee identiteiten hebben, Auth.Id en Global Identity Policy, met authenticatie ingeschakeld op Auth.Id Identity.

De volgende stap is om de Auth.Id Identity te gebruiken en toegangsbeleid te maken op basis van deze Identiteit. U kunt de gewenste AD-groepen of gebruikers opgeven in het toegangsbeleid.

-
1. Kies GUI > Web Security Manager > Toegangsbeleid.
 2. Klik op Beleid toevoegen.
 3. Volg deze stappen om een toegangsbeleid te maken:
 1. Beleidsnaam: Sales.Policy
 2. boven beleid invoegen: 1
 3. Identiteitsbeleid: Auth.Id - Geautoriseerde groepen en gebruikers opgeven

4. Voer de groepsnamen handmatig in of klik op Vernieuwingsmap om de lijst met gebruikers op uw advertentie te zien. Klik op Toevoegen als u de gebruikers hebt geselecteerd.
5. Klik op Indienen als u klaar bent.

Als u een ander toegangsbeleid moet maken, klikt u op Beleid toevoegen en maakt u een ander toegangsbeleid voor de nieuwe AD-groep.

U dient geen nieuwe identiteiten aan te maken voor hetzelfde verificatieterrein. Hergebruik de bestaande identiteit (Auth.Id) en creëer nieuw toegangsbeleid voor verschillende AD-groepen, zolang de identiteit niet is gebonden aan Proxy-poorten, URL-categorieën, gebruikersagents of Leden definiëren op Subnet.

Voor meervoudig toegangsbeleid met verschillende AD-groepen moet de installatie er als volgt uitzien:

Identiteit

"Auth.id"

"Mondiaal identiteitsbeleid"

Toegangsbeleid

Verkoop.beleid met behulp van "Auth.id"

"Support.Policy" via "Auth.ID"

"Manager.Policy" via "Auth.Id"

"Admin.Policy" via "Auth.Id"

"Mondiaal beleid" met behulp van "Alle"

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.