

Beveiligde clientdistributiemethoden voor veilige toegang tot RAVPN

Inhoud

uitgifte

Bij het configureren van externe vendortoegang tot Remote Access VPN (RAVPN) in Cisco Secure Access hebben beheerders een methode nodig waarmee leveranciers de AnyConnect/Secure Client-software kunnen downloaden. In tegenstelling tot eerdere ASA-implementaties waarbij de VPN-URL directe clientdownloads bood, bieden Cisco Secure Access VPN-headend-URL's geen clientdownloadfunctie. Deze beperking is van invloed op het onboardingproces voor externe leveranciers die externe toegangsmogelijkheden nodig hebben.

Beheerders verwachten dat de VPN-setup-URL's binnen Secure Access leveranciers toegang verlenen om de AnyConnect-client te downloaden, vergelijkbaar met het gedrag dat eerder beschikbaar was bij ASA-gebaseerde implementaties waarbij de VPN-URL clientdownloads zou toestaan voordat verbinding wordt gemaakt.

milieu

- Cisco Secure Access met RAVPN-configuratie
- Toegangsvereisten voor externe leveranciers
- Migratie van ASA-gebaseerde VPN-implementatie
- Distributiebehoeften AnyConnect/Secure Client

resolutie

Cisco Secure Access host geen Secure Client-pakketten op de URL's van de VPN-kop. De

oplossing maakt gebruik van hostscantechnologie in plaats van directe clientdownloads via de VPN-URL. Als u de Secure Client-software wilt distribueren naar externe leveranciers, gebruikt u een van deze goedgekeurde methoden.

Methode 1: Dashboarddistributie voor beveiligde toegang

1.- Verkrijg installatiepakketten rechtstreeks van het Dashboard voor beveiligde toegang voor handmatige distributie.

2.- Navigeer naar Eindgebruikersconnectiviteit en klik op de knop Cisco Secure Client om installatiepakketten te downloaden voor distributie naar leveranciers.

Methode 2: Cisco Software Download Site

Leveranciers kunnen pakketten rechtstreeks downloaden als ze de juiste rechten hebben:

- Leverancier moet een Cisco-account met softwarerechten hebben
- Toegang tot pakketten via software.cisco.com
- Vereist planning vóór implementatie en installatie van Cisco-account van leverancier

Methode 3: handmatige distributie

De Secure Client-software handmatig of via alternatieve distributiekanaalen buiten de VPN-URL naar externe leveranciers distribueren. Deze methode biedt de meeste controle over het distributieproces en vereist geen Cisco-accounts van leveranciers.

Oorzaak

Cisco Secure Access VPN headend URL's zijn anders ontworpen dan ASA-gebaseerde implementaties. De Secure Access-oplossing host geen clientinstallatiepakketten op de koppen en

maakt in plaats daarvan gebruik van hostscantechnologie. Dit architecturale verschil betekent dat de VPN-URL's niet dezelfde clientdownloadfunctionaliteit kunnen bieden die beschikbaar was bij ASA-implementaties.

Gerelateerde inhoud

- [Cisco Technical Support en downloads](#)

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.