Umbrella Roaming Client configureren op een bedrijfsnetwerk

Inhoud

Inleiding

In dit document wordt de configuratie van de Umbrella-roamingclient in uw bedrijfsnetwerk beschreven.

Overzicht

De Umbrella-roamingclient is een geweldig hulpmiddel voor het beschermen van externe gebruikers, maar het kan ook gebruikers op uw bedrijfsnetwerk beschermen en een andere beveiligingslaag toevoegen. Afhankelijk van de behoeften van het bedrijf willen sommige beheerders de bescherming van de Umbrella-roamingclient op het bedrijfsnetwerk voortzetten, terwijl andere beheerders de Umbrella-roamingclient liever 'terugzetten' ten gunste van andere Umbrella-beleidsregels.

Umbrella biedt flexibiliteit in de manier waarop de Umbrella-roamingclient werkt wanneer deze uw netwerk binnenkomt. In dit artikel worden deze verschillende benaderingen beschreven.

Doelen

V). Waarom zou ik de Umbrella-roamingclient op mijn bedrijfsnetwerk uitschakelen?

Het is normaal gesproken niet nodig om de Umbrella-roamingclient uit te schakelen om interne en externe DNS te laten werken. De Umbrella-roamingclient gebruikt de functie Domeinbeheer om uw interne DNS-verkeer naar uw normale DNS-servers te leiden. Hierdoor kunt u zowel bescherming als connectiviteit behouden terwijl de Umbrella-roamingclient op uw eindpunten op het netwerk wordt uitgevoerd.

Er zijn echter soms redenen om te overwegen de bescherming van de roamingclient uit te schakelen...

- Een ander beleid voor '*on-network*' en '*off-network*' aanbieden aan roamende gebruikers die het netwerk verlaten.
- Het gebruik van een interne DNS-server op een bedrijfsnetwerk biedt enkele voordelen op het gebied van caching en verminderd uitgaand DNS-verkeer.
- De Umbrella-roamingclient verzendt periodiek sondeberichten om de verbinding met Umbrella te verifiëren. Dit extra verkeer kan ongewenst zijn wanneer u een zeer groot aantal klanten hebt.

V) Waarom zou ik willen dat de Umbrella-roamingclient ingeschakeld blijft op mijn bedrijfsnetwerk?

Aan de andere kant zijn er enkele zeer goede redenen om de roamingclient te allen tijde ingeschakeld te houden:

- Zorg ervoor dat de Umbrella roaming-clientcomputer te allen tijde hetzelfde beleid gebruikt.
- Altijd de hostnaam van de Umbrella-roamingclient identificeerbaar in rapporten (in plaats van de netwerkidentiteit) - voor gedetailleerde rapportage.
- De Roaming Client gebruikt 'Encrypted DNS'-verkeer voor meer privacy
- Voor gebruikers van Secure Web Gateway (die AnyConnect gebruiken) moet de client ingeschakeld blijven om SWG-webfilters te kunnen leveren.

werkingsmodi

Altijd AAN

De Umbrella-roamingclient kan blijven ingeschakeld, zelfs wanneer deze wordt gebruikt op het bedrijfsnetwerk. In deze modus worden beleidsregels geconfigureerd met behulp van de Umbrella-clientidentiteit voor roaming. Deze identiteit wordt weergegeven in rapporten.

Beleid	De Umbrella roaming client Identity wordt altijd gebruikt.
verslaggeving	De Umbrella roaming client Identity wordt altijd weergegeven in rapporten met granulariteit per machine
DNS-verkeer	• De Umbrella-roamingclient blijft DNS-query's rechtstreeks naar Umbrella verzenden, zelfs wanneer deze zich op een bedrijfsnetwerk bevindt. • Query's die naar Umbrella worden verzonden, zijn gecodeerd en bieden extra beveiliging.

	• Query's voor 'Interne domeinen' worden gerouteerd naar uw normale DNS-servers en niet naar Umbrella verzonden.
Probe Berichten	De Umbrella-roamingclient blijft sondeberichten verzenden om de beschikbaarheid van Umbrella te bepalen.

Hoe configureer ik de 'Always ON'-modus:

1. Navigeer naar Identiteiten > Zwervende computers.
2. Klik op het pictogram (Zwervende clientinstellingen).
3. Schakel DNS-omleiding uit terwijl u zich in een beschermd netwerk bevindt en klik op Opslaan.
4. Maak een apart beleid voor uw Umbrella-roamingklanten en zorg ervoor dat dit de hoogste prioriteit heeft (de allerhoogste prioriteit). Uw overkoepelende roamingclientbeleid moet een hogere prioriteit hebben dan elk beleid op basis van netwerkidentiteiten.

Regelmatig netwerkbeleid gebruiken
De Umbrella-roamingclient is ingeschakeld en blijft rechtstreeks met Umbrella praten, maar de netwerkidentiteit wordt gebruikt voor zowel beleids- als rapportagedoeleinden. Deze modus wordt geactiveerd door het netwerkbeleid een hogere prioriteit toe te kennen dan het beleid voor roamingclients van Umbrella.

Beleid	Het netwerkbeleid wordt gebruikt wanneer u zich op het beveiligde netwerk bevindt. Dit maakt verschillende aan/uit-netwerkbeleidsregels mogelijk.
verslaggeving	• Rapportage is gekoppeld aan de netwerkidentiteit als de primaire identiteit. • Met rapportage kunt u nog steeds zoeken via de hostnaam van de Umbrella-roamingclient om alleen resultaten voor die client te filteren. 

DNS-verkeer	• De Umbrella-roamingclient blijft DNS-query's rechtstreeks naar Umbrella verzenden, zelfs wanneer deze zich op een bedrijfsnetwerk bevindt. • Query's die naar Umbrella worden verzonden, zijn gecodeerd en bieden extra beveiliging. • Query's voor 'Interne domeinen' worden gerouteerd naar uw normale DNS-servers en niet naar Umbrella verzonden.
Probe Berichten	De Umbrella-roamingclient blijft sondeberichten verzenden om de beschikbaarheid van Umbrella te bepalen.

Hoe 'Regelmatig netwerkbeleid gebruiken':

1. Navigeer naar Identiteiten > Zwervende computers.
2. Klik op het pictogram (Zwervende clientinstellingen).
3. Schakel DNS-omleiding uit terwijl u zich in een beschermd netwerk bevindt en klik op Opslaan.
4. Maak een apart beleid voor uw netwerk(en). Zorg ervoor dat het beleid voor uw netwerk(en) een hogere prioriteit heeft dan het beleid op basis van de roamingclient.

Schakel achter beveiligde netwerken uit (ideaal voor kleinere netwerken)
De Umbrella-roamingclient kan 'terugschakelen' wanneer deze detecteert dat deze zich op een beveiligd netwerk bevindt. Dit betekent dat Network Identity wordt gebruikt voor zowel beleids- als rapportagedoeleinden.

Deze modus is qua gedrag vergelijkbaar met de modus 'Regelmatig netwerkbeleid gebruiken', behalve dat de Umbrella-roamingclient zichzelf uitschakelt en het DNS-verkeer niet verstoort.

Beleid	Het netwerkbeleid wordt gebruikt wanneer u zich op het beveiligde netwerk bevindt. Dit maakt verschillende aan/uit-netwerkbeleidsregels mogelijk.
verslaggeving	Op het beveiligde netwerk is er geen granulariteit per machine voor de rapportage. Rapportage is alleen gekoppeld aan de netwerkidentiteit.
DNS-verkeer	Wanneer op het beveiligde netwerk de Umbrella roaming client niet interfereert met DNS queries en ze gaan naar de normale interne DNS-server.

Probe Berichten	De Umbrella-roamingclient blijft probe-berichten verzenden om te bepalen of deze zich op een beveiligd netwerk bevindt.

Configureren Uitschakelen achter beveiligde netwerken:

1. Navigeer naar Identiteiten > Zwervende computers.
2. Klik op het pictogram (Zwervende clientinstellingen).
3. Selecteer DNS-omleiding uitschakelen terwijl u zich in een overkoepelend beveiligd netwerk bevindt en klik op Opslaan.
4. Navigeer naar Beleid > Beleidslijst.
5. Maak een apart beleid voor uw netwerk(en). Zorg ervoor dat het beleid voor uw netwerk(en) een hogere prioriteit heeft dan het beleid op basis van de Umbrella-roamingclient.
6. Uw lokale DNS-servers moeten worden doorgestuurd naar Umbrella resolvers en moeten correct worden geregistreerd in het Umbrella-dashboard.
7. Om deze functie te laten werken, moet de IP-uitgang die door het clientwerkstation wordt gebruikt, worden geregistreerd op dezelfde netwerkidentiteit als de IP-uitgang die door uw interne DNS-servers wordt gebruikt. Voor volledige details, zie dit artikel.

Schakel het vertrouwde netwerkdomein uit (ideaal voor grotere netwerken)

Het is nu mogelijk om een door de klant geconfigureerd 'Trusted Network Domain' te kiezen. De client probeert dit DNS-domein (A-record) op te lossen en de beveiliging uit te schakelen wanneer het domein met succes wordt opgelost. Dit is bedoeld als een intern DNS-record dat alleen wordt opgelost wanneer de client zich in het bedrijfsnetwerk bevindt.

Beleid	De client maakt een back-off wanneer het vertrouwde domein wordt gedetecteerd en ontvangt niet noodzakelijkerwijs het overkoepelende beleid of de filters. We raden aan om andere Umbrella-functies toe te voegen (bijv. netwerkbeveiliging) om ervoor te zorgen dat het beleid nog steeds wordt toegepast op het bedrijfsnetwerk.
verslaggeving	De client maakt een back-off wanneer het vertrouwde domein wordt gedetecteerd en ontvangt niet noodzakelijkerwijs het overkoepelende beleid of de filters. Als het netwerk wordt beschermd door andere overkoepelende functies (bijvoorbeeld netwerkbeveiliging), wordt het verkeer weergegeven in rapporten onder de netwerkidentiteit.
DNS-verkeer	Wanneer op het vertrouwde netwerk de Umbrella roaming client niet interfereren met DNS queries en ze gaan naar de normale interne DNS-server.

Probe Berichten	De Umbrella-roamingclient schakelt het merendeel van zijn DNS-probe-tests in deze staat uit, waardoor de hoeveelheid verkeer die door roamingclients wordt gegenereerd, aanzienlijk wordt verminderd.

Hoe configureert u Trusted Network Domain:

1. Maak een DNS-A-record op uw interne DNS-servers (bijv. magic.mydomain.tld).
    1. Het record moet een "subdomein" zijn (minimaal 3 DNS-labels)
    2. Het record moet worden opgelost in een intern RFC-1918-adres
    3. Zorg ervoor dat het record niet publiekelijk bestaat
2. Navigeer naar Identiteiten > Zwervende computers.
3. Klik op het pictogram (Zwervende clientinstellingen).
4. Selecteer de optie Trusted Network Domain en voer de domeinnaam in (bijv. magic.mydomain.tld). Klik op Save (Opslaan).

De Umbrella Roaming-client gebruiken met een overkoepelend virtueel apparaat

Als onderdeel van het Umbrella 'Insights'-product (in de pakketten Platform en Insights) bieden we een Virtual Appliance (VA) aan die fungeert als een DNS-forwarder binnen uw netwerk. Deze VA is de sleutel tot het verkrijgen van inzicht in de bron van DNS-verzoeken op uw netwerk en is ook vereist voor onze Active Directory-integratie.

Standaard schakelt de Umbrella-roamingclient zichzelf uit als deze detecteert dat een VA wordt gebruikt voor DNS-doorgifte. Als de VA is toegewezen als de DNS-server (met behulp van DHCP- of statische instellingen), detecteert de Umbrella-roamingclient dit en schakelt deze zichzelf uit.

VA Backoff

Beleid	Met VA Backoff ingeschakeld, wordt de VA Identity gebruikt om het gekozen beleid te bepalen. Beleid kan worden gemaakt op basis van deze identiteiten: • AD-gebruiker (alleen als AD-integratie is ingeschakeld) • AD Computer (alleen als AD-integratie is ingeschakeld) • intern netwerk • Naam van de overkoepelende site. Klik hier voor meer informatie over beleidsprioriteit.
verslaggeving	Als VA Backoff is ingeschakeld, is de Umbrella-roamingclient uitgeschakeld achter een VA en wordt deze niet weergegeven in rapporten. Rapportage

	wordt geregistreerd als: • AD-gebruiker (alleen als AD-integratie is ingeschakeld) • AD Computer (alleen als AD-integratie is ingeschakeld) • intern netwerk • Naam van de overkoepelende site. Daarnaast wordt het interne client-IP-adres voor elk verzoek geregistreerd. 
DNS-verkeer	• De Umbrella roaming-client interfereert niet met DNS-query's en ze gaan naar het virtuele apparaat. • De VA stuurt externe DNS-query's door naar Umbrella (versleuteld). • De VA routeert interne DNS-query's naar gelang van het geval en stuurt deze door naar de geconfigureerde interne DNS-servers.
Probe Berichten	De Umbrella roaming client stuurt nog steeds probe berichten naar Umbrella, maar doet dit tegen een gereduceerd tarief.

Hoe VA Backoff te configureren:

1. Deze functie is standaard ingeschakeld, maar u kunt de status controleren (en deze optioneel uitschakelen)
2. Navigeer naar Identiteiten > Zwervende computers.
3. Klik op het pictogram (Zwervende clientinstellingen).
4. Selecteer de optie VA-back-off

Cisco Umbrella AnyConnect-beveiligingsmodule voor roaming

De overkoepelende module voor Cisco AnyConnect ondersteunt alle dezelfde werkingsmodi als hierboven beschreven. Er zijn ook twee extra specifieke AnyConnect-modi beschikbaar. Beide modi kunnen worden ingeschakeld in uw overkoepelende dashboard op de pagina Identiteiten > Zwervende computers, maar er is aanvullende configuratie vereist in het AnyConnect VPN-profiel.

- Respecteer AnyConnect Trusted Network Detection.
  Deze functie zorgt ervoor dat de Umbrella Security-module wordt uitgeschakeld wanneer Cisco AnyConnect bepaalt dat de module zich op een vertrouwd netwerk bevindt. Dit is afhankelijk van de functie Vertrouwde netwerkdetectie van AnyConnect om het netwerk te identificeren. Vertrouwde domeinen, DNS-servers en URL's kunnen worden gebruikt om uw bedrijfsnetwerk te identificeren. Zie de AnyConnect-documentatie voor meer informatie.
- Schakel Roaming Client uit terwijl volledige VPN-tunnelsessies actief zijn

Als deze functie is ingeschakeld, wordt de overkoepelende module uitgeschakeld wanneer AnyConnect is verbonden met een VPN voor de volledige tunnel (of alle DNS-tunnels).

Wanneer de Zwervende client is uitgeschakeld, filtert deze geen DNS-verkeer. Het is dus belangrijk om ervoor te zorgen dat uw netwerk wordt gedekt door andere beveiligingsfuncties, zoals de functie Netwerkbeveiliging.

Meer informatie

Als u de roamingclient op uw bedrijfsnetwerk wilt uitschakelen, maar meer controle nodig hebt of andere opties wilt bespreken, neemt u contact op met Cisco Umbrella Support.

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.