IPS-decodering controleren in Cisco Secure Access

Inhoud

uitgeven

Bij het gebruik van Cisco Secure Access met RAVPN (Remote Access VPN) via Secure Client moeten organisaties controleren of IPS (Intrusion Prevention System)-decodering en -inspectie correct worden uitgevoerd voor verkeer naar specifieke websites. De primaire uitdaging is om te bevestigen dat TLS-decodering en inspectieprocessen goed functioneren via andere methoden dan de standaard UI-logboeken voor beheer, zoals Activity Search. Specifieke verificatievereisten omvatten het identificeren van certificaatcontroles aan de clientzijde of foutopsporings-/rapportagemechanismen die testvalidatie kunnen ondersteunen en aanvullende bevestiging van IPS-werking kunnen bieden buiten de beheerinterface.

milieu

- Cisco Secure Access (CSA) met RAVPN-functionaliteit
- Cisco Secure Client voor VPN-verbindingen met externe toegang
- Mogelijkheden voor IPS-decodering en -inspectie ingeschakeld
- TLS/SSL-verkeer waarvoor decodering vereist is voor beveiligingsinspectie
- Webverkeer van RAVPN-clients naar externe websites

resolutie

Er zijn twee methoden om te controleren of IPS-decodering en -inspectie correct werken voor VPN-verkeer met externe toegang in Cisco Secure Access:

Methode 1: zoeken naar activiteiten via beheerinterface (primaire methode)

De functie Activity Search in de beheerinterface van Cisco Secure Access biedt de meest betrouwbare methode om IPS-decodering en inspectiebewerkingen te bevestigen. Deze interface geeft gedetailleerde logboeken en analyses weer die laten zien wanneer het verkeer is gedecodeerd en geïnspecteerd door de beveiligingsdiensten.

Toegang tot Activiteit zoeken:

Navigeer naar het Cisco Secure Access-beheerdashboard en zoek de functionaliteit voor het zoeken naar activiteiten om de verkeersinspectielogs en de decoderingsstatus voor specifieke gebruikerssessies en bestemmingswebsites te bekijken.

Als u decoderingslogs wilt inschakelen, kunt u deze instelling inschakelen voor algemene instellingen:

Dashboard -> Veilig -> Toegangsbeleid -> Regelstandaardinstellingen en algemene instellingen -> Globale instellingen -> Decryptielogboek.

Methode 2: Verificatie van het clientcertificaat

Als extra verificatiemethode kunt u certificaatcontroles aan de clientzijde uitvoeren om te bevestigen dat het verkeer wordt ontsleuteld.

Wanneer Cisco Secure Access met succes TLS-verkeer decodeert en inspecteert, presenteert het zijn eigen certificaat aan de client in plaats van het oorspronkelijke websitecertificaat.

Om decodering te controleren door middel van certificaatinspectie:

1. Controleer het websitecertificaat
Open de certificaatgegevens in de browser en bekijk de uitgever en de geldigheidsperiode.

Als het certificaat is uitgegeven door Cisco Secure Access Root CA met een geldigheidsduur van ~ 10 dagen, geeft dit de decodering van het inbraakpreventiesysteem op firewallniveau aan.

Als de geldigheid van het certificaat ongeveer 5 dagen is, geeft dit Secure Web Gateway-gebaseerde decodering aan.

2. De certificaatuitgever valideren (gelijknamige naam)

Deze verificatiemethode voor certificaten aan de clientzijde dient als een aanvullende bevestigingstechniek naast de primaire methode voor zoeken naar activiteiten en biedt extra zekerheid dat de IPS-decoderingsprocessen naar verwachting functioneren.

Inbraakpreventiesysteem decoderen niet:

Decodering voor Intrusion Prevention System gaat plaatsvinden als -

· Het is ingeschakeld onder globale instellingen EN

· Inbraakpreventiesysteem is ingeschakeld voor ten minste één van de regels van het toegangsbeleid (ik ben van mening dat hoewel de regel is uitgeschakeld, deze voorwaarde nog steeds van toepassing is)

Wilt u een domein omzeilen van Intrusion Prevention System-decodering

Gebruik het meegeleverde systeem niet decoderen lijst en voeg domein toe in het geleverde systeem niet decoderen lijst.

of

Brongebaseerde decodering gebruiken onder Globale instellingen voor Cisco Secure-toegang -

OPMERKING: Dit werkt als er GEEN uitgaande NAT is geconfigureerd in de netwerktunnelconfiguratie voor beveiligde toegang.

Oorzaak

De noodzaak van meerdere verificatiemethoden vloeit voort uit de vereiste om de handhaving van het beveiligingsbeleid in bedrijfsomgevingen te valideren. Hoewel UI-logboeken voor beheer een uitgebreide zichtbaarheid bieden, bieden verificatiemethoden aan de clientzijde extra bevestigingspunten die nuttig kunnen zijn voor nalevingstests, probleemoplossing en validatiescenario's waarbij directe toegang tot beheerinterfaces beperkt kan zijn of wanneer meerdere verificatiepunten vereist zijn voor grondige testprocedures.

Verwante 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.