Verduidelijking van de impact op de prestaties en best practices voor SSL/TLS-decodering op FTD

Inhoud

uitgifte

Een gebruiker is van plan SSL/TLS-decodering in te schakelen op een Firewall Threat Defense (FTD)-apparaat en moet de potentiële impact op de prestaties van het apparaat begrijpen voordat het wordt geïmplementeerd. Belangrijke aandachtspunten zijn onder meer:

- Impact op firewalldoorvoer, latentie en algemene prestaties van de verkeersverwerking.
- Het verwachte CPU- en geheugengebruik neemt toe na het inschakelen van decodering.
- Richtlijnen en prestatiebenchmarks voor de grootte van specifieke FTD-modellen.
- Aanbevolen limieten voor gelijktijdige gedecodeerde sessies.
- Best practices en vereisten voor de implementatie van de productie.

milieu

- Vuurkracht 4115. Ook andere hardwareplatforms kunnen worden getroffen.
- FTD versie 7.4.2 (build 172). Ook andere softwareversies kunnen worden beïnvloed.
- Overweging voor SSL/TLS-decodering.
- Implementatieplanning van productieomgeving.

resolutie

SSL / TLS-decryptie voegt verwerkingsoverhead toe aan de Firepower 4115, maar de werkelijke impact hangt sterk af van hoeveel verkeer wordt ontsleuteld en welke inspectie wordt toegepast na decryptie.

Prestatie-effectbeoordeling

De effecten van SSL/TLS-decryptie omvatten:

- Lagere effectieve doorvoer.
- Hogere latentie.
- Verhoogd CPU-gebruik voor snort/inspectie.
- CPU- en geheugentoename die niet nauwkeurig kan worden voorspeld als een vast percentage zonder analyse van het echte verkeersprofiel.

FPR 4115 Prestatiebenchmarks

Cisco's gepubliceerde Firepower 4115-benchmarkspecificaties:

- TLS-hardwaredecoderingsdoorvoer: 6,5 Gbps.
- FW + AVC-doorvoer: 33 Gbps.
- Maximale gelijktijdige sessies met AVC: 15 miljoen.
- Maximale nieuwe aansluitingen per seconde met AVC: 210K.

Belangrijke opmerking over de grootte: de 6,5 Gbps TLS-hardwaredecoderingsbenchmark is gebaseerd op specifieke testomstandigheden. De productiedoorvoer kan lager zijn als u een groot percentage van het verkeer decodeert, ontsleuteld verkeer inspecteert met Intrusion / File / Malware-beleid of veel kortstondige TLS-sessies verwerkt.

Cisco publiceert geen afzonderlijk nummer voor "maximale gelijktijdige gedecodeerde sessies" voor Firepower 4115 op FTD 7.4.2. In de praktijk wordt de capaciteit gevalideerd met behulp van de verkeersmix, gelijktijdige sessies, verbindingssnelheid, coderingssuites en de belasting van het

inspectiebeleid.

Aanbevolen aanpak voor productie-implementatie

Stap 1: Begin met een beperkte pilot

- Schakel in eerste instantie geen brede "decrypt all" -regels in.
- Begin met geselecteerde gebruikers, subnetten of doelcategorieën.
- Houd de standaardverwerking conservatief met Niet decoderen voor verkeer waarvoor geen inspectie vereist is.

Stap 2: Verkeer uitsluiten dat vaak breekt met decryptie

- Banken/financiële sites.
- portalen voor gezondheidszorg.
- Toepassingen met een certificaat.
- Sommige Software as a Service (SaaS) en endpoint security/cloud applicaties.
- Gevoelige bedrijfskritieke toepassingen, tenzij expliciet getest.

Stap 3: Houd SSL-regels eenvoudig en zorgvuldig geordend

- Plaats specifieke Do Not Decrypt-uitsluitingen boven bredere decryptieregels.
- Vermijd overdreven brede of complexe matching waar mogelijk.
- Gebruik geen TLS-versie of cipher-suite-voorwaarden voor Decrypt-Design/Known-Key-regels, omdat Cisco-documenten dit onvoorspelbaar gedrag kunnen veroorzaken.

Stap 4: Gereedheid van certificaat valideren

- Voor uitgaande Decrypt-Resign moet het ondertekenende CA-certificaat worden vertrouwd door client-eindpunten.

- Voor inbound Known-Key decryptie moet de firewall beschikken over het juiste servercertificaat/private key materiaal.

Stap 5: Monitor tijdens de uitrol

- Volg het totale CPU-gebruik en, nog belangrijker, het gebruik van de Snort/Inspection CPU.
- Volg gelijktijdige verbindingen en nieuwe verbindingen per seconde.
- Controleer de SSL-stroomstatus/handshake-fouten in verbindingsgebeurtenissen.
- Let op TLS-overinschrijvingsindicatoren en toepassingsspecifieke storingen.

Voor meer informatie over het controleren van de CPU:

- https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2026/pdf/BRKSEC-2362.pdf
- Think Like a TAC Engineer: Een gids voor Cisco Secure Firewall meest voorkomende pijnpunten

Voor het bijhouden van verbindingen en nieuwe verbindingen per seconde controleert u:

- Aanbevolen procedures bij logboekregistratie

Voor het bijhouden van SSL-stroomstatus/handdruk-fouten in verbindingsgebeurtenissen controleert u de TLS-indicatoren voor overinschrijving:

- Overabonnement op TLS/SSL oplossen

Stap 6: Rol terug of smal bereik als u ziet:

- Aanhoudende inspectie CPU verzadiging.
- Door de gebruiker zichtbare latentie wordt verhoogd.
- TLS-handdruk mislukt.
- Zakelijke toepassingen mislukken na decryptie.
- Overmatig abonnement of overmatige SSL-fouten.

Stap 7: Overweeg de impact van TLS 1.3

TLS 1.3 kan de zichtbaarheid en het gedrag beïnvloeden, omdat bepaalde handdruk- en inspectiekenmerken verschillen van TLS 1.2.

Oorzaak

Voor het decoderen van SSL/TLS zijn extra computationele middelen nodig om verkeersstromen te decoderen, te inspecteren en opnieuw te coderen. De impact op de prestaties varieert aanzienlijk op basis van verkeerspatronen, inspectiebeleid toegepast op ontsleuteld verkeer en de specifieke implementatieconfiguratie. Zonder goede planning en geleidelijke implementatie kunnen organisaties onverwachte prestatiedegradatie ervaren in productieomgevingen.

Gerelateerde inhoud

- Handleiding voor apparaatconfiguratie van Cisco Secure Firewall Management Center - Decryptieregels
- Cisco Secure Firewall Decryption Policy Guidance
- Best Practice voor Decryption Policy Rule Order
- Vereenvoudiging van decodering met Cisco's Secure Firewall 7.7
- Beste praktijken voor decoderingsregels
- Gegevensoverzicht Cisco Firepower 4100-reeks
- 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.