Cisco IOS fysieke firewall/IPS: Het configureren van context-gebaseerde toegangscontrole (CBAC) voor Denial-of-Service bescherming

Inhoud

Inleiding

Dit document beschrijft de tuning procedure voor de parameters Denial of Service (DoS) in de Cisco IOS Classic Firewall met CBAC.

CBAC biedt geavanceerde filterfuncties voor het verkeer en kan worden gebruikt als een integraal onderdeel van uw netwerkfirewall.

DoS verwijst over het algemeen naar netwerkactiviteit die ofwel opzettelijk ofwel onbedoeld de netwerkbronnen overweldigt zoals WAN-linkbandbreedte, tabellen voor firewallverbinding, end-host geheugen, CPU of servicemogelijkheden. In het slechtst denkbare scenario overweldigt de activiteit van DoS het kwetsbare (of gerichte) middel tot het punt dat het middel niet beschikbaar wordt, en het verbiedt WAN connectiviteit of de diensttoegang tot legitieme gebruikers.

De Cisco IOS Firewall kan bijdragen aan de verzachting van de DoS-activiteit als het tellers van het aantal "half-open" TCP-verbindingen onderhoudt, evenals het totale verbindingstarief via de firewall- en inbraakpreventiesoftware in zowel Classic Firewall (**ip-inspectie**) als Zone-Based Policy Firewall.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Half-open verbindingen zijn TCP verbindingen die niet de drierichtings SYN-SYN/ACK-ACK handdruk hebben voltooid die altijd door TCP peers wordt gebruikt om de parameters van hun wederzijdse verbinding te onderhandelen. Grote aantallen half-open verbindingen kunnen wijzen op kwaadwillige activiteit, zoals DoS of Distributed-denial-of-service (DDoS) aanvallen. Een voorbeeld van één type van de aanval van Dos wordt uitgevoerd door kwaadaardige, opzettelijk ontwikkelde software, zoals wormen of virussen die meerdere hosts op het internet infecteren en proberen specifieke servers van Internet met SYN-aanvallen te overweldigen, waar grote aantallen SYN-verbindingen naar een server worden verzonden door meerdere hosts op het internet of binnen het privénetwerk van een organisatie. SYN-aanvallen vormen een gevaar voor internetservers omdat de verbindingstabellen van servers kunnen worden geladen met "bogus" SYN-aansluitingen die sneller arriveren dan de server met de nieuwe verbindingen kan omgaan. Dit is een type DoS-aanval omdat het grote aantal verbindingen in de TCP-verbindingslijst van de slachtoffer server de legitieme toegang van de gebruiker tot de slachtoffer Internet-servers onmogelijk maakt.

Cisco IOS Firewall ziet ook USDatagram Protocol-sessies (UDP) met verkeer in slechts één richting als 'half-open' omdat veel toepassingen die UDP gebruiken voor transport de ontvangst van gegevens erkennen. UDP sessies zonder retourverkeer zijn waarschijnlijk een indicatie van DoS-activiteit of pogingen om verbinding te maken tussen twee hosts, waarbij een van de hosts geen respons heeft vertoond. Veel soorten UDP-verkeer, zoals logberichten, SNMP-netwerkbeheerverkeer, streaming spraak- en videomedia en signaleringsverkeer, gebruiken alleen verkeer in één richting om hun verkeer over te brengen. Veel van deze types van verkeer passen toepassingsspecifieke intelligentie toe om unidirectionele verkeerspatronen te verhinderen het gedrag van firewalls en IPS DoS negatief te beïnvloeden.

Vóór Cisco IOS-softwarerelease 12.4(11)T en 12.4(10) biedt Cisco IOS stateful Packet inspection bescherming tegen DoS-aanvallen als standaard wanneer een inspectieregel werd toegepast. Cisco IOS-softwarerelease 12.4(11)T en 12.4(10)hebben de standaardinstellingen van het DOS zodanig gewijzigd dat de DoS-beveiliging niet automatisch wordt toegepast, maar de tellers van de verbindingsactiviteit zijn nog steeds actief. Wanneer DoS protection actief is, d.w.z. wanneer de standaardwaarden gebruikt worden bij oudere softwarereleases, of wanneer de waarden aangepast zijn aan de bereik die het verkeer beïnvloeden, wordt DoS-beveiliging ingeschakeld op de interface waar de inspectie wordt uitgevoerd, in de richting waarin de firewall wordt toegepast, zodat de configuratieprotocollen voor het firewallbeleid kunnen worden geïnspecteerd. DoS-

beveiliging is alleen ingeschakeld op het netwerkverkeer als het verkeer een interface invoert of verlaat met een inspectie die in dezelfde richting van het oorspronkelijke verkeer wordt uitgevoerd (SYN-pakket of eerste UDP-pakket) voor een TCP- of UDP-sessie.

Cisco IOS-firewallinspectie biedt verschillende instelbare waarden om te beschermen tegen DoS-aanvallen. Cisco IOS-softwarereleases vóór 12.4(11)T en 12.4(10) hebben standaard DoS-waarden die de juiste netwerkwerking kunnen verstoren als ze niet zijn ingesteld voor het juiste niveau van netwerkactiviteit in netwerken waar de verbindingssnelheden de standaardwaarden overschrijden. Deze parameters staan u toe om de punten te vormen waarop de DoS bescherming van uw firewallrouter van kracht wordt. Wanneer de Dos tellers van uw router de standaard of de gevormde waarden overschrijden, stelt de router één oude half-open verbinding voor elke nieuwe verbinding terug die de geconfigureerde max-incomplete of één-minuut hoge waarden overschrijdt tot het aantal half-open sessies onder de maximum-incomplete lage waarden daalt. De router verstuurt een syslogbericht als houtkap is ingeschakeld en als een IPS (Inbraakpreventiesysteem) op de router is ingesteld, stuurt de firewallrouter een DoS-signatuur-bericht via de Security Devices Exchange (SDEE). Als de DoS-parameters niet aangepast zijn aan het normale gedrag van uw netwerk, kan de normale netwerkactiviteit het DoS-beschermingsmechanisme activeren, waardoor toepassingsfouten, slechte netwerkprestaties en een hoog CPU-gebruik op de Cisco IOS-firewallrouter worden veroorzaakt.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Denial-of-service tuning voor Cisco IOS-software, cloudfirewall (IP-inspectie) en inbraakpreventiesysteem

De klassieke Cisco IOS Firewall behoudt een globale reeks DoS tellers voor de router, en alle firewallsessies voor alle firewallbeleid op alle interfaces worden toegepast op de algemene reeks firewalltellers.

Cisco IOS Clastic Firewall Inspection biedt bescherming tegen DoS-aanval standaard wanneer een Clastic Firewall wordt toegepast. Wordt de S-beveiliging ingeschakeld op alle interfaces waar de inspectie wordt uitgevoerd, in de richting waarin de firewall wordt toegepast, voor elke service of protocol dat het firewallbeleid is geconfigureerd voor inspectie. Classic Firewall biedt verschillende aanpasbare waarden om te beschermen tegen DoS-aanvallen. De standaardinstellingen van de nalatenschap (van softwarebeelden vóór release 12.4(11)T) die in Tabel 1 worden getoond, kunnen interfereren met de juiste netwerkwerking als ze niet zijn geconfigureerd voor het juiste niveau van netwerkactiviteit in netwerken waar de aansluittarieven de standaardinstellingen overschrijden. De instellingen DoS kunnen met de exec opdracht worden bekeken **tonen IP inspect alle**, en de instellingen zijn opgenomen met de output van **sh ip inspecteert alle**.

CBAC gebruikt tijdelijke instellingen en drempels om te bepalen hoe lang het beheer van staatsinformatie voor een sessie duurt, en om te bepalen wanneer sessies die niet volledig worden geïnstalleerd moeten worden laten vallen. Deze tijdelijke instellingen en drempels gelden wereldwijd voor alle sessies.

Tabel 1 Standaard VoS-beveiligingslimieten voor klassieke firewall		
DoS-beschermingswaarde	**Vóór 12.4(11)T/12.4(10)**	**12.4(11)T/12.4(10) en later**
max-incomplete hoge *waarde*	500	Onbeperkt
max-incomplete lage *waarde*	400	Onbeperkt
hoge *waarde* van één minuut	500	Onbeperkt
lage *waarde* van één minuut	400	Onbeperkt
tcp max-incomplete host *waarde*	50	Onbeperkt

Routers die zijn ingesteld om Cisco IOS VRF-bewuste firewall toe te passen, onderhouden één verzameling tellers voor elke VRF.

De teller voor "ip inspecteert een minuut hoog" en "ip inspecteert een minuut laag" onderhoudt een som van alle pogingen van de verbinding van TCP-, UDP- en Internet Control Message Protocol (ICMP) binnen de minuut voorafgaand aan de bediening van de router, of de verbindingen al dan niet succesvol zijn geweest. Een stijgende verbindingssnelheid kan wijzen op een worminfectie op een privénetwerk of een poging tot een DoS-aanval tegen een server.

Terwijl u de DoS-beveiliging van uw firewall niet kunt "uitschakelen", kunt u de DoS-beveiliging aanpassen zodat deze niet van kracht wordt, tenzij er een zeer groot aantal half-open verbindingen aanwezig zijn in de sessietabel van uw firewallrouter.

DoS-firewallbescherming

Volg deze procedure om de DoS-bescherming van uw firewall af te stemmen op de activiteit van uw netwerk:

1. Zorg ervoor dat uw netwerk niet is geïnfecteerd met virussen of wormen die kunnen leiden tot onjuist grote halfopen verbindingswaarden of poging tot verbindingssnelheden. Als uw netwerk niet "schoon" is, is er geen manier om de DoS-bescherming van uw firewall goed aan te passen. U moet de activiteit van uw netwerk binnen een periode van typische activiteit waarnemen. Als u de VVV-beveiligingsinstellingen van uw netwerk binnen een periode van lage of stille netwerkactiviteit instelt, worden de beveiligingsinstellingen van de VVV waarschijnlijk overschreden.
2. Stel de max-incomplete hoge waarden in op zeer hoge waarden:

   ```
   ip inspect max-incomplete high 20000000
   ip inspect one-minute high 100000000
   ip inspect tcp max-incomplete host 100000 block-time 0
   ```

   Dit voorkomt dat de router DoS bescherming biedt terwijl u de verbindingspatronen van uw netwerk observeert. Als u de DoS-bescherming wilt uitschakelen, stopt u deze

procedure.**N.B.:** Als uw router Cisco IOS-softwarerelease 12.4(11)T of hoger, of 12.4(10) of hoger, hoeft u de standaardwaarden voor DoS-bescherming niet te verhogen. zij zijn al standaard aan hun maximumgrenzen gebonden .**Opmerking:** Als u de agressievere TCP host-specifieke denial-of-service preventie wilt inschakelen die de blokkering van verbindingsinitiatie naar een host omvat, moet u de bloktijd instellen die in de **IP-inspectie** is gespecificeerd**, max-incomplete host** opdracht

3. Schakel de Cisco IOS-firewallstatistieken met deze opdracht uit:

   ```
   show ip inspect statistics reset
   ```

4. Laat de router in deze toestand enige tijd configureren, misschien wel tot 24 tot 48 uur, zodat u het netwerkpatroon kunt observeren gedurende ten minste één volledige dag van de typische cyclus van netwerkactiviteit.**Opmerking:** Hoewel de waarden op zeer hoge niveaus zijn ingesteld, profiteert uw netwerk niet van de Cisco IOS-firewall of IPS DoS-bescherming.
5. Controleer na de observatieperiode de DokS-tellers met deze opdracht:

   ```
   show ip inspect statistics
   ```

   De parameters die u moet waarnemen om de DoS-beveiliging op te stellen, worden **vet** gemarkeerd:

   ```
   Packet inspection statistics
      [process switch:fast switch]
     tcp packets: [218314:7878692]
     udp packets: [501498:65322]
      packets: [376676:80455]
      packets: [5738:4042411]
     smtp packets: [11:11077]
     ftp packets: [2291:0]
   Interfaces configured for inspection 2
   Session creations since subsystem
      startup or last reset 688030
   Current session counts
      (estab/half-open/terminating) [0:0:0]
   Maxever session counts
      (estab/half-open/terminating) [207:56:35]
   Last session created 00:00:05
   Last statistic reset never
   Last session creation rate 1
   Maxever session creation rate 330
   Last half-open session total 0
   TCP reassembly statistics
     received 46591 packets out-of-order; dropped 16454
     peak memory usage 48 KB; current usage: 0 KB
     peak queue length 16
   ```

6. Configureer **ip inspectie max-incomplete hoge** waarde 25% hoger dan de aangegeven maximale sessie tellen half-open waarde van uw router. Een 1,25-multiplier biedt 25% hoofdruimte boven het waargenomen gedrag, bijvoorbeeld:

   ```
   Maxever session counts
      (estab/half-open/terminating) [207:56:35]
   56 * 1.25 = 70
   ```

   Configureren:

   ```
   router(config)
      #ip inspect max-incomplete high 70
   ```

   Opmerking: Dit document beschrijft het gebruik van een multiplier van 1.25 keer de typische

activiteit van uw netwerk om grenzen in te stellen om de VoS-bescherming in te zetten. Als u uw netwerk binnen typische pieken van de netwerkactiviteit observeert, moet dit voldoende bewegingsruimte bieden om de DoS-bescherming van de router onder alle behalve atypische omstandigheden te voorkomen. Als uw netwerk regelmatig grote uitbarstingen van legitieme netwerkactiviteit ziet die deze waarde overschrijden, voert de router de DoS beschermingsmogelijkheden aan die een negatieve impact op een aantal van het netwerkverkeer kunnen veroorzaken. U moet uw routerlogbestanden controleren op detectie van DoS-activiteit en de **ip-inspectie** aanpassen **max-onvolledig hoog** en/of **ip inspecteert een minuut-**hoge limieten om **het** starten van DoS te voorkomen, nadat u hebt vastgesteld dat de limieten zijn aangetroffen als resultaat van legitieme netwerkactiviteit. U kunt de DoS-beveiligingstoepassing herkennen op basis van log-berichten zoals deze:

7. Configureer **ip inspecteert max-incomplete lage** tot de waarde die uw router voor zijn maximale sessielenaantal half-open waarde **toont**, bijvoorbeeld:

   ```
   Maxever session counts
      (estab/half-open/terminating) [207:56:35]
   ```

   Configureren:

   ```
   router(config)
      #ip inspect max-incomplete low 56
   ```

8. De teller voor **ip inspecteert een minuut hoog** en **een minuut laag** een som van alle TCP-, UDP- en Internet Control Message Protocol (ICMP)-verbindingspogingen binnen de minuut voorafgaand aan de routerhandeling, of de verbindingen al dan niet succesvol zijn geweest. Een stijgende verbindingssnelheid kan wijzen op een worminfectie op een privénetwerk, of een poging tot een DoS-aanval tegen een server. Er werd een extra inspectiestatistiek toegevoegd aan de **inspectiestatistieken** van **de** toonaangevende ip in 12.4(11)T en 12.4(10) om het hoge watermerk voor het aantal sessies bekend te maken. Als u een Cisco IOS-softwarerelease eerder dan 12.4(11)T of 12.4(10) runt, bevatten de inspectiestatistieken deze regel niet:

   ```
   Maxever session creation rate [value]
   ```

   Cisco IOS-softwarereleases vóór 12.4(11)T en 12.4(10) houden geen waarde voor een maximale verbindingssnelheid van één minuut in, dus u moet de waarde berekenen die u toepast op basis van waargenomen waarden voor de 'meestersessie'. Opmerkingen van verschillende netwerken die de stateful inspection van Cisco IOS Firewall release 12.4(11)T in productie gebruiken hebben aangetoond dat de Maxever sessies creatie rentetarieven de som van de drie waarden (vastgesteld, half open en eindigend) in "maximum sessielocatie" met grofweg tien procent overschrijden. Om de ip-waarde te berekenen, moet de aangegeven "vastgestelde" waarde met 1.1 worden vermenigvuldigd, bijvoorbeeld:

   ```
   Maxever session counts
      (estab/half-open/terminating) [207:56:35]
   (207 + 56 + 35) * 1.1 = 328
   ```

   Configureren:

   ```
   ip inspect one-minute low 328
   ```

   Als de router Cisco IOS-softwarerelease 12.4(11)T of later, of 12.4(10) of hoger draait, kunt u simpelweg de waarde toepassen die wordt weergegeven in de inspectiestatistiek "Max. sessiecreëersnelheid":

   ```
   Maxever session creation rate 330
   ```

   Configureren:

   ```
   ip inspect one-minute low 330
   ```

9. Bereken en configureren **ip inspecteert een minuut hoog**. De ip inspecteert een hoge waarde van één minuut moet 25% hoger zijn dan de berekende een-minuut-waarde, bijvoorbeeld:

   ```
   ip inspect one-minute low (330) * 1.25 = 413
   ```

Configureren:

```
ip inspect one-minute high 413
```

Opmerking: Dit document beschrijft het gebruik van een multiplier van 1.25 keer de typische activiteit van uw netwerk om grenzen in te stellen om de VoS-bescherming in te zetten. Als u uw netwerk binnen typische pieken van de netwerkactiviteit observeert, moet dit voldoende bewegingsruimte bieden om de DoS-bescherming van de router onder alle behalve atypische omstandigheden te voorkomen. Als uw netwerk regelmatig grote uitbarstingen van legitieme netwerkactiviteit ziet die deze waarde overschrijden, voert de router de DoS beschermingsmogelijkheden aan die een negatieve impact op een aantal van het netwerkverkeer kunnen veroorzaken. U moet uw routerlogbestanden controleren op detectie van DoS-activiteit en de **ip-inspectie** aanpassen **max-onvolledig hoog** en/of **ip inspecteert een minuut-**hoge limieten om **het** starten van DoS te voorkomen, nadat u hebt vastgesteld dat de limieten zijn aangetroffen als resultaat van legitieme netwerkactiviteit. U kunt de DoS-beveiligingstoepassing herkennen op basis van log-berichten zoals deze:

10. U moet een waarde definiëren voor **IP-inspectie van tcp max-incomplete host** in overeenstemming met uw kennis van de capaciteit van uw servers. Dit document kan geen richtlijnen bieden voor de configuratie per host van de DOS-beveiliging, aangezien deze waarde sterk varieert op basis van de hardware- en softwareprestaties van de eindgebruiker. Als u niet zeker bent over de juiste grenzen voor de configuratie van de DOS-beveiliging, hebt u effectief twee opties om de Dos-limieten te definiëren:De verkiesbare optie is om op router gebaseerde DoS-bescherming tegen een hoge waarde (onder of gelijk aan de maximale waarde van 4.294.967.295) te configureren en host-specifieke bescherming toe te passen die door het besturingssysteem van elke host of een extern host-gebaseerd inbraakbeschermingssysteem zoals Cisco Security Agent (CSA) wordt geboden.Onderzoek activiteit en prestatilogbestanden op uw netwerkhosts en bepalen hun pieksnelheid van de duurzame verbinding. Omdat de Klastische Firewall slechts één globale teller aanbiedt, moet u de maximum waarde toepassen die u bepaalt nadat u alle netwerkhosts controleert op hun maximale verbindingssnelheden. Het is nog steeds raadzaam om OS-specifieke activiteitslimieten en een op host gebaseerde IPS zoals CSA te gebruiken.**Opmerking:** Cisco IOS-firewall biedt beperkte bescherming tegen gerichte aanvallen op specifieke besturingssystemen en toepassingskwetsbaarheden. De DoS-bescherming van de Cisco IOS-firewall biedt geen bescherming tegen compromis op end-host services die worden blootgesteld aan potentieel vijandige omgevingen.
11. Controleer de beveiligingsactiviteit van uw netwerk. Idealiter moet u een syslogserver of idealiter een Cisco Monitoring and Reporting Stations (MARS) gebruiken om voorvallen van de DoS-aanvaldetectie op te nemen. Als de detectie heel vaak gebeurt, moet u uw DoS-beveiligingsparameters bewaken en aanpassen.Voor meer informatie over de aanvallen van TCP SYN DoS, verwijs naar het definiëren van strategieën om te beschermen tegen TCP SYN Denial of Service aanvallen.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Cisco PIX-firewallsoftware
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Security meldingen uit het veld (inclusief PIX)
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems