ASA-functionaliteit en -configuratie voor bedreigingsdetectie vaststellen

Inhoud

Inleiding

In dit document worden de drie belangrijkste onderdelen van de functionaliteit en configuratie voor bedreigingsdetectie beschreven.

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document beschrijft de functionaliteit en basisconfiguratie van de optie Threat Detection van de Cisco adaptieve security applicatie (ASA). Threat Detection biedt firewallbeheerders de nodige tools om aanvallen te identificeren, te begrijpen en te stoppen voordat ze de interne netwerkinfrastructuur bereiken. Om dit te doen steunt de eigenschap op een aantal verschillende triggers en statistieken, die in detail worden beschreven in deze secties.

Bedreigingsdetectie kan worden gebruikt op elke ASA-firewall die een softwareversie van 8.0(2) of hoger uitvoert. Hoewel detectie van bedreigingen geen vervanging is voor een speciale IDS/IPS-oplossing, kan deze worden gebruikt in omgevingen waar geen IPS beschikbaar is om een extra beschermingslaag te bieden voor de kernfunctionaliteit van ASA.

Functionaliteit voor bedreigingsdetectie

De optie voor detectie van bedreigingen heeft drie hoofdcomponenten:

1. Basis bedreigingsdetectie
2. Geavanceerde detectie van bedreigingen
3. Bedreigingsdetectie scannen

Elk van deze componenten wordt in detail beschreven in deze secties.

Basisdetectie van bedreigingen (tarieven op systeemniveau)

Basis detectie van bedreigingen is standaard ingeschakeld op alle ASA's die 8.0(2) en hoger uitvoeren.

De basis bedreigingsopsporing controleert de tarieven waarbij de pakketten om diverse redenen door ASA als geheel worden gelaten vallen. Dit betekent dat de statistieken die door de detectie van basisbedreigingen worden gegenereerd, alleen van toepassing zijn op het gehele apparaat en over het algemeen niet korrelig genoeg zijn om informatie te verschaffen over de bron of de specifieke aard van de bedreiging. In plaats daarvan lieten de ASA-monitoren pakketten voor deze gebeurtenissen vallen:

- ACL Drop (ACL-drop) - pakketten worden ontkend door toegangslijsten.
- Bad Pkts (bad-packet-drop) - ongeldige pakketformaten, waaronder L3- en L4-headers die niet voldoen aan RFC-standaarden.
- Conn Limit (conn-limit-drop) - pakketten die een geconfigureerde of wereldwijde verbindingslimiet overschrijden.
- DoS-aanval (dos-drop) - DoS-aanvallen (Denial of Service).
- Firewall (fw-drop) - basiscontroles voor firewalls.
- ICMP-aanval (ICMP-drop) - verdachte ICMP-pakketten.
- Inspecteer (inspect-drop) - Denial by application inspection.
- Interface (interface-drop) - pakketten die door interfacecontroles worden gelaten vallen.
- Scannen (scannen-bedreigend) - netwerk-/hostscanaanvallen.
- SYN Attack (syn-attack) - Onvolledige sessieaanvallen, waaronder TCP/SYN-aanvallen en unidirectionele UDP-sessies die geen terugkeergegevens hebben.

Elk van deze gebeurtenissen heeft een specifieke set triggers die worden gebruikt om de bedreiging te identificeren. De meeste triggers zijn gekoppeld aan specifieke ASP drop redenen, hoewel bepaalde syslogs en inspectie acties ook worden overwogen. Sommige triggers worden bewaakt door meerdere bedreigingscategorieën. Een aantal van de meest voorkomende triggers worden in deze tabel beschreven, alhoewel het geen uitputtende lijst is:

Basis bedreigingen	Trigger(s) / ASP Drop Reason(s)
bel-drop	bel-drop
slechte pakket-drop	ongeldig-tcp-hdr-lengte ongeldige IP-header inspect-dns-pak-te-lang inspect-dns-id-not-matching
conn-limit-drop	limiet
droppen	Sp-beveiliging is mislukt
foudruppel	inspecteren-icmp-seq-num-niet-overeenkomend inspect-dns-pak-te-lang inspect-dns-id-not-matching Sp-beveiliging is mislukt bel-drop
ICMP-drop	inspecteren-icmp-seq-num-niet-overeenkomend
inspectiedrupp	Framedruppels geactiveerd door een inspectiemotor
interface-drop	Sp-beveiliging is mislukt zonder route
scandreiging	TCP-3whs-negatief TCP niet-syn Sp-beveiliging is mislukt bel-drop inspecteren-icmp-seq-num-niet-overeenkomend inspect-dns-pak-te-lang inspect-dns-id-not-matching
syn-aanval	%ASA-6-302014 syslog met demontage reden van "SYN Time-out"

Voor elke gebeurtenis, de fundamentele bedreigingsopsporing meet de tarieven dat deze dalingen over een gevormde periode van tijd voorkomen. Deze periode wordt het gemiddelde snelheidsinterval (ARI)

genoemd en kan variëren van 600 seconden tot 30 dagen. Als het aantal gebeurtenissen dat zich binnen de ARI voordoet de ingestelde snelheidsdrempels overschrijdt, beschouwt de ASA deze gebeurtenissen als een bedreiging.

De basis bedreigingsopsporing heeft twee configureerbare drempels voor wanneer het gebeurtenissen als een bedreiging beschouwt: het gemiddelde tarief en het barsttarief. Het gemiddelde tarief is simpelweg het gemiddelde aantal druppels per seconde binnen de tijdsperiode van de geconfigureerde ARI. Als bijvoorbeeld de gemiddelde drempelwaarde voor ACL-dalingen is ingesteld op 400 met een ARI van 600 seconden, berekent de ASA het gemiddelde aantal pakketten dat in de afgelopen 600 seconden door ACLâ€™s is gevallen. Als dit aantal groter blijkt te zijn dan 400 per seconde, registreert ASA een bedreiging.

Op dezelfde manier is de burst rate zeer vergelijkbaar, maar kijkt naar kleinere periodes van snapshot data, genaamd de burst rate interval (BRI). De BRI is altijd kleiner dan de ARI. Voortbouwend op het vorige voorbeeld, de ARI voor ACL-druppels is nog 600 seconden en heeft nu een burst rate van 800. Met deze waarden berekent de ASA het gemiddelde aantal pakketten dat door ACLâ€™s in 20 seconden wordt weergegeven, waarbij 20 seconden het BRI is. Als deze berekende waarde meer dan 800 druppels per seconde overschrijdt, wordt een bedreiging vastgelegd. Om te bepalen welke BRI wordt gebruikt, berekent de ASA de waarde van 1/30th van de ARI. Daarom in het eerder gebruikte voorbeeld, 1/30th van 600 seconden is 20 seconden. De detectie van bedreigingen heeft echter een minimale BRI van 10 seconden, dus als 1/30th van de ARI minder dan 10 is, gebruikt de ASA nog steeds 10 seconden als de BRI. Ook is het belangrijk op te merken dat dit gedrag verschilde in versies voorafgaand aan 8.2(1), die een waarde van 1/60th van de ARI gebruikte, in plaats van 1/30th. De minimum BRI van 10 seconden is hetzelfde voor alle softwareversies.

Wanneer een basisbedreiging wordt gedetecteerd, genereert de ASA eenvoudigweg syslog %ASA-4-733100 om de beheerder te waarschuwen dat een potentiële bedreiging is gedetecteerd. Het gemiddelde, het huidige en het totale aantal gebeurtenissen voor elke bedreigingscategorie kan worden gezien met de opdracht **voor** het **detecteren van** de **showbedreiging**. Het totale aantal cumulatieve gebeurtenissen is de som van het aantal gebeurtenissen dat in de laatste 30 BRI-steekproeven is gezien.

De barstsnelheid in syslog wordt berekend op basis van het aantal pakketten dat tot nu toe in de huidige BRI is gelaten vallen. De berekening wordt periodiek gemaakt in een BRI. Wanneer een breuk optreedt, wordt een syslog opgehoogd. Het is beperkt dat slechts één syslog in een BRI wordt geproduceerd. De barstsnelheid in "show bedreigingsdetectie rate" wordt berekend op basis van het aantal pakketten dat in laatste BRI is gelaten vallen. Het ontwerp voor het verschil is dat syslog tijdgevoelig is zodat als een breuk in huidige BRI gebeurt, het een kans zou hebben om worden gevangen. "toon bedreigingsopsporingssnelheid" is minder tijdgevoelig, zodat het nummer van laatste BRI wordt gebruikt.

De fundamentele bedreigingsopsporing voert geen acties om het afwijkende verkeer tegen te houden of toekomstige aanvallen te verhinderen. In deze zin is de opsporing van basisbedreigingen louter informatief en kan zij worden gebruikt als monitoring- of rapportagemechanisme.

Geavanceerde detectie van bedreigingen (statistieken op objectniveau en boven-N)

In tegenstelling tot Basic Threat Detection, kan Advanced Threat Detection worden gebruikt om statistieken voor meer korrelige objecten bij te houden. ASA ondersteunt trackingstatistieken voor host IPâ€™s, poorten, protocollen, ACLâ€™s en servers die worden beschermd door TCP-onderschepping. Geavanceerde detectie van bedreigingen is alleen standaard ingeschakeld voor ACL-statistieken.

Voor host, poort en protocol objecten houdt Threat Detection het aantal pakketten, bytes en druppels bij die zowel verzonden als ontvangen zijn door dat object binnen een specifieke tijdsperiode. Voor ACLâ€™s houdt Threat Detection de top 10 van ACEâ€™s (zowel vergunning als ontkenning) bij die het meest zijn geraakt binnen een bepaalde periode.

In al deze gevallen wordt 20 minuten, 1 uur, 8 uur en 24 uur gewacht. Hoewel de tijdsperioden zelf niet configureerbaar zijn, kan het aantal periodes dat per object wordt bijgehouden worden aangepast met het sleutelwoord 'aantal snelheden'. Zie het gedeelte Configuration voor meer informatie. Als bijvoorbeeld 'number-of-rate' is ingesteld op 2, zie je alle statistieken voor 20 minuten, 1 uur en 8 uur. Als 'number-of-rate' is ingesteld op 1, zie je alle statistieken voor 20 minuten, 1 uur. Hoe dan ook, de 20-minutenkoers wordt altijd weergegeven.

Als TCP-onderschepping is ingeschakeld, kan Threat Detection de top 10-servers bijhouden die worden beschouwd als onder aanval en beschermd door TCP-onderschepping. Statistieken voor TCP-onderschepping zijn vergelijkbaar met Basic Threat Detection in de zin dat de gebruiker het gemeten snelheidsinterval kan configureren samen met specifieke gemiddelde (ARI) en burst (BRI) snelheden. Geavanceerde statistieken voor detectie van bedreigingen voor TCP-onderschepping zijn alleen beschikbaar in ASA 8.0(4) en hoger.

De geavanceerde statistieken van de Opsporing van de Bedreiging worden bekeken via de **show bedreigingsopsporing statistieken** en **tonen bedreigingsopsporing statistieken hoogste** bevelen. Dit is ook de functie verantwoordelijk voor de populatie van de "top" grafieken op het firewall dashboard van ASDM. De enige syslogs die worden gegenereerd door Advanced Threat Detection zijn %ASA-4-733104 en %ASA-4-733105, die worden geactiveerd wanneer de gemiddelde en burst snelheden (respectievelijk) worden overschreden voor TCP-onderscheppingsstatistieken.

Net zoals Basic Threat Detection is de Advanced Threat Detection puur informatief. Er worden geen acties uitgevoerd om verkeer te blokkeren op basis van de statistieken voor geavanceerde detectie van bedreigingen.

Bedreigingsdetectie scannen

Scannen Threat Detection wordt gebruikt om bij te houden van vermoedelijke aanvallers die verbindingen maken met te veel hosts in een subnetverbinding of veel poorten op een host/subnetverbinding. Scannen Threat Detection is standaard uitgeschakeld.

Scannen Threat Detection bouwt voort op het concept Basic Threat Detection, die al een bedreigingscategorie definieert voor een scanaanval. Daarom worden de instellingen voor het snelheidsinterval, het gemiddelde tarief (ARI) en de burst rate (BRI) gedeeld tussen de basisinstellingen en de instellingen voor scannen van bedreigingen. Het verschil tussen de 2 functies is dat terwijl Basic Threat Detection alleen aangeeft dat de gemiddelde of burst rate drempels werden gekruist, Scanning Threat Detection een database van aanvaller en doel IP-adressen onderhoudt die kan helpen om meer context rond de hosts die betrokken zijn bij de scan. Bovendien wordt alleen verkeer dat daadwerkelijk wordt ontvangen door de doelhost/subnetbeheerder beschouwd door detectie van bedreigingen scannen. Basisdetectie van bedreigingen kan nog steeds een scandreiging activeren, zelfs als het verkeer door een ACL wordt gedropt.

Scannen Threat Detection kan optioneel op een aanval reageren door de aanvaller IP te overschaduwen. Dit maakt Scanning Threat Detection de enige subset van de Threat Detection-functie die actief verbindingen via de ASA kan beïnvloeden.

Wanneer detectie van bedreigingen door scannen een aanval detecteert, wordt %ASA-4-733101 gelogd op de aanvaller en/of doel-IP's. Als de functie is ingesteld om de aanvaller uit te schakelen, wordt %ASA-4-733102 vastgelegd als er een melding wordt gegenereerd tijdens het scannen van bedreigingsdetectie. %ASA-4-733103 wordt gelogd wanneer de haak is verwijderd. De opdracht **scanning**-bedreigingsdetectie voor **show** kan worden gebruikt om de gehele Scanning Threat database te bekijken.

Beperkingen

- Threat Detection is alleen beschikbaar in ASA 8.0(2) en hoger. Het wordt niet ondersteund op het

ASA 1000V-platform.
- Bedreigingsdetectie wordt alleen ondersteund in één contextmodus.
- Er worden alleen "zonder doos"-bedreigingen gedetecteerd. Verkeer dat naar de ASA zelf wordt verzonden, wordt niet in aanmerking genomen bij bedreigingsdetectie.
- TCP-verbindingspogingen die door de beoogde server zijn hersteld, worden niet geteld als een SYN-aanval of Scanning-bedreiging.

Configuratie

Basis bedreigingsdetectie

Basic Threat Detection is ingeschakeld met de opdracht **Threat Detection Basic-Threat**.

<#root>

```
ciscoasa(config)#
```

threat-detection basic-threat

De standaardsnelheden kunnen worden bekeken met de opdracht **Alle bedreigingen opsporen uitvoeren**.

<#root>

```
ciscoasa(config)#
```

show run all threat-detection

```
threat-detection rate dos-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate dos-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate bad-packet-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate bad-packet-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate acl-drop rate-interval 600 average-rate 400 burst-rate 800
threat-detection rate acl-drop rate-interval 3600 average-rate 320 burst-rate 640
threat-detection rate conn-limit-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate conn-limit-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate icmp-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate icmp-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate scanning-threat rate-interval 600 average-rate 5 burst-rate 10
threat-detection rate scanning-threat rate-interval 3600 average-rate 4 burst-rate 8
threat-detection rate syn-attack rate-interval 600 average-rate 100 burst-rate 200
threat-detection rate syn-attack rate-interval 3600 average-rate 80 burst-rate 160
threat-detection rate fw-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate fw-drop rate-interval 3600 average-rate 320 burst-rate 1280
threat-detection rate inspect-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate inspect-drop rate-interval 3600 average-rate 320 burst-rate 1280
threat-detection rate interface-drop rate-interval 600 average-rate 2000 burst-rate 8000
threat-detection rate interface-drop rate-interval 3600 average-rate 1600 burst-rate 6400
```

Om deze tarieven met douanewaarden te stemmen, configureer eenvoudig het bevel van de **bedreigingsopsporing tarief** voor de aangewezen bedreigingscategorie aan.

<#root>

```
ciscoasa(config)#
```

```
threat-detection rate acl-drop rate-interval 1200 average-rate 250 burst-rate 550
```

Elke bedreigingscategorie kan maximaal 3 verschillende tarieven hebben (met tarief ID's van tarief 1, tarief 2, en tarief 3). De overschrijding van de specifieke snelheids-ID wordt in de syslog %ASA-4-733100 aangegeven.

In het vorige voorbeeld, leidt de bedreigingsopsporing tot syslog 733100 slechts wanneer het aantal ACL dalingen 250 dalingen/seconde over 1200 seconden of 550 dalingen/seconde over 40 seconden overschrijdt.

Geavanceerde detectie van bedreigingen

Gebruik de opdracht **statistieken voor bedreigingsdetectie** om geavanceerde detectie van bedreigingen mogelijk te maken. Als geen specifiek eigenschapsleutelwoord wordt verstrekt, laat het bevel het volgen voor alle statistieken toe.

<#root>

```
ciscoasa(config)#
```

```
threat-detection statistics ?
```

```
configure mode commands/options:
 access-list      Keyword to specify access-list statistics
 host            Keyword to specify IP statistics
 port            Keyword to specify port statistics
 protocol       Keyword to specify protocol statistics
 tcp-intercept   Trace tcp intercept statistics
 <cr>
```

Om het aantal snelheidsintervallen te vormen die voor gastheer, haven, protocol, of ACL statistieken worden gevolgd, gebruik het **aantal-van-tarief** sleutelwoord.

<#root>

```
ciscoasa(config)#
```

```
threat-detection statistics host number-of-rate 2
```

Het sleutelwoord voor het aantal snelheden configureert bedreigingsdetectie om alleen het kortste *aantal* intervallen te volgen.

Om TCP-onderscheppingsstatistieken in te schakelen, gebruikt u de opdracht **TCP-onderschepping voor** bedreigingsdetectie.

<#root>

```
ciscoasa(config)#
```

```
threat-detection statistics tcp-intercept
```

Om douanetarieven voor de onderscheppingsstatistieken van TCP te vormen, gebruik het **tarief-interval**, het **gemiddelde tarief**, en de **burst-rate** sleutelwoorden.

```
<#root>

ciscoasa(config)#

threat-detection statistics tcp-intercept rate-interval 45 burst-rate 400 average-rate 100
```

Bedreigingsdetectie scannen

Gebruik de opdracht **scanning-**bedreigingsdetectie om **scanning-**bedreigingsdetectie in te schakelen.

```
<#root>

ciscoasa(config)#

threat-detection scanning-threat
```

Als u de snelheden voor een scandreiging wilt aanpassen, gebruikt u dezelfde opdracht voor de **detectie van bedreigingen** die wordt gebruikt door de basisdetectie van bedreigingen.

```
<#root>

ciscoasa(config)#

threat-detection rate scanning-threat rate-interval 1200 average-rate 250 burst-rate 550
```

Om ASA in staat te stellen een IP-scanaanval af te sluiten, voegt u het **schuine** trefwoord toe aan de opdracht **scanning-**bedreigingsdetectie.

```
<#root>

ciscoasa(config)#

threat-detection scanning-threat shun
```

Hiermee kan Scanning Threat Detection een één uur durende shun voor de aanvaller maken. Gebruik de opdracht **duur** van **scanning-**bedreigingsdetectie om **de** duur van de **shun aan te** passen.

```
<#root>

ciscoasa(config)#

threat-detection scanning-threat shun duration 1000
```

In sommige gevallen kunt u voorkomen dat de ASA bepaalde IPâ€™s verwaarloost. Om dit te doen, moet u een uitzondering maken met de **schuintrekken van scandreigingen voor detectie van bedreigingen, behalve** opdracht.

<#root>

```
ciscoasa(config)#
```

```
threat-detection scanning-threat shun except ip-address 10.1.1.1 255.255.255.255
```

```
ciscoasa(config)#
```

```
threat-detection scanning-threat shun except object-group no-shun
```

Prestaties

Basic Threat Detection heeft zeer weinig invloed op de prestaties van de ASA. Geavanceerde en Scannen Threat Detection zijn veel meer bron-intensief omdat ze moeten bijhouden van verschillende statistieken in het geheugen. Alleen Threat Detection scannen met de functie Shun ingeschakeld kan actief invloed hebben op verkeer dat anders zou zijn toegestaan.

Naarmate de ASA softwareversies zich verder hebben ontwikkeld, is het geheugengebruik van Threat Detection aanzienlijk geoptimaliseerd. Er moet echter op worden gelet dat het geheugengebruik van ASA wordt bewaakt voordat en nadat Threat Detection is ingeschakeld. In sommige gevallen, zou het beter zijn om bepaalde statistieken (bijvoorbeeld, host statistieken) tijdelijk alleen toe te laten terwijl u actief problemen oplossen van een specifiek probleem.

Voor een gedetailleerdere weergave van het geheugengebruik van Threat Detection voert u de opdracht **show memory app-cache bedreigingsdetectie [detail]** uit.

Aanbevolen acties

Deze secties geven een aantal algemene aanbevelingen voor acties die kunnen worden ondernomen wanneer verschillende dreigingsdetectiegerelateerde gebeurtenissen zich voordoen.

Wanneer een Basic Drop Rate wordt overschreden en %ASA-4-733100 wordt gegenereerd

Bepaal de specifieke bedreigingscategorie die wordt vermeld in de syslog %ASA-4-733100 en correleer dit met de output van show threat-detection rate . Controleer met deze informatie de uitvoer van show asp drop om de redenen te bepalen waarom het verkeer is weggevallen.

Voor een gedetailleerdere weergave van verkeer dat om een specifieke reden wordt gedropt, gebruikt u een ASP-drop-opname met de reden in kwestie om alle pakketten te zien die worden gedropt. Bijvoorbeeld, als ACL Drop-bedreigingen worden vastgelegd, vastleggen op de ASP drop-reden van acl-drop :

<#root>

```
ciscoasa#
```

```
capture drop type asp-drop acl-drop
```

```
ciscoasa#
```

```
show capture drop
```

```
1 packet captured

   1: 18:03:00.205189 10.10.10.10.60670 > 192.168.1.100.53:  udp 34 Drop-reason:
 (acl-drop) Flow is denied by configured rule
```

Deze opname laat zien dat het gedropte pakket een UDP/53-pakket van 10.10.10.10 tot 192.168.1.100 is.

Als %ASA-4-733100 een scandreiging meldt, kan het ook handig zijn om tijdelijk de detectie van bedreigingen door scannen in te schakelen. Dit staat ASA toe om spoor van de bron en de bestemming IPs te houden betrokken bij de aanval.

Aangezien Basic Threat Detection voornamelijk verkeer controleert dat al door de ASP is weggelaten, is er geen directe actie vereist om een potentiële bedreiging te stoppen. De uitzonderingen hierop zijn SYN-aanvallen en scanbedreigingen, die betrekking hebben op verkeer dat door de ASA verloopt.

Als de druppels die worden gezien in de ASP-drop-opname legitiem zijn en/of verwacht worden voor de netwerkomgeving, stemmen de basissnelheidsintervallen af op een meer geschikte waarde.

Als de druppels illegaal verkeer laten zien, moeten er acties worden ondernomen om het verkeer te blokkeren of te beperken voordat het de ASA bereikt. Dit kan ACLâ€™s en QoS op upstream-apparaten omvatten.

Bij SYN-aanvallen kan verkeer in een ACL op de ASA worden geblokkeerd. TCP-onderschepping kan ook worden geconfigureerd om de beoogde server(s) te beschermen, maar dit kan eenvoudigweg resulteren in een Conn Limit-bedreiging die in plaats daarvan wordt vastgelegd.

Voor het scannen van bedreigingen kan verkeer ook worden geblokkeerd in een ACL op de ASA. Dreigingsdetectie scannen met de shunDe optie kan worden ingeschakeld om de ASA toe te staan om alle pakketten voor een bepaalde periode proactief te blokkeren van de aanvaller.

Wanneer een scandreiging wordt gedetecteerd en %ASA-4-733101 wordt vastgelegd

%ASA-4-733101 moet een lijst maken van de doelhost/subnetserver of het IP-adres van de aanvaller. Controleer voor de volledige lijst van doelen en aanvallers de output van show threat-detection scanning-threat.

Packet-opnamen op de ASA-interfaces die met de aanvaller worden geconfronteerd en/of het doelwit of de doelwitten kunnen ook helpen de aard van de aanval te verduidelijken.

Als de gedetecteerde scan een niet-verwachte scan is, moeten er maatregelen worden genomen om het verkeer te blokkeren of te beperken voordat het de ASA bereikt. Dit kan ACLâ€™s en QoS op upstream-apparaten omvatten. Wanneer de shunDe optie wordt toegevoegd aan de Scanning Threat Detection. Hiermee kan de ASA proactief alle pakketten van de aanvaller IP laten vallen voor een bepaalde periode. Als laatste redmiddel kan het verkeer ook handmatig op de ASA worden geblokkeerd via een ACL- of TCP-onderscheppingsbeleid.

Als de gedetecteerde scan vals positief is, stel de intervallen voor de scanning Threat rate dan in op een

geschiktere waarde voor de netwerkomgeving.

Wanneer een aanvaller is uitgeschakeld en %ASA-4-733102 is vastgelegd

%ASA-4-733102 geeft het IP-adres van de afgebakende hacker weer. Gebruik de show threat-detection shun bevel om een volledige lijst van aanvallers te bekijken die specifiek door de Detectie van de Bedreiging zijn gemeden. Gebruik de show shun opdracht om de volledige lijst weer te geven van alle IPâ€™s die actief door de ASA worden gemeden (dit omvat andere bronnen dan detectie van bedreigingen).

Als de schijn deel uitmaakt van een legitieme aanval, is er geen verdere actie vereist. Echter, het zou nuttig zijn om het verkeer van de aanvaller zo ver mogelijk naar de bron te blokkeren. Dit kan via ACLâ€™s en QoS. Dit zorgt ervoor dat intermediaire apparaten geen middelen hoeven te verspillen aan illegaal verkeer.

Als de Scanning dreiging die de shun teweegbracht een vals positief was, verwijder handmatig de shun met de clear threat-detection shun [IP_address] uit.

Wanneer %ASA-4-733104 en/of %ASA-4-733105 is vastgelegd

%ASA-4-733104 en %ASA-4-733105 maakt een lijst van de host waarop de aanval is gericht en die momenteel wordt beschermd door TCP-onderschepping. Voor meer informatie over de aanvalssnelheden en beschermde servers, controleer de uitvoer van show threat-detection statistics top tcp-intercept .

<#root>

ciscoasa#

show threat-detection statistics top tcp-intercept

```
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245  Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

Wanneer Advanced Threat Detection een aanval van deze aard detecteert, beschermt de ASA de beoogde server al via TCP-onderschepping. Controleer de ingestelde verbindingslimieten om ervoor te zorgen dat ze voldoende bescherming bieden voor de aard en snelheid van de aanval. Ook zou het voordelig zijn om het verkeer van de aanvaller zo ver mogelijk stroomopwaarts naar de bron te blokkeren. Dit kan via ACLâ€™s en QoS. Dit zorgt ervoor dat intermediaire apparaten geen middelen hoeven te verspillen aan illegaal verkeer.

Als de gedetecteerde aanval vals positief is, pas dan de tarieven voor een TCP-onderscheppingsaanval aan op een meer geschikte waarde met de threat-detection statistics tcp-interceptuit.

Hoe een bedreiging handmatig te activeren

Om te testen en problemen op te lossen, kan het nuttig zijn om handmatig verschillende bedreigingen te activeren. Deze sectie bevat tips over hoe u een aantal veel voorkomende bedreigingstypen kunt activeren.

Basis bedreigingen - ACL-drop, firewall en scannen

Raadpleeg de tabel in het vorige gedeelte Functionaliteit om een bepaalde Basis Threat te activeren. Kies een specifieke ASP-reden en verstuur verkeer door de ASA dat zou worden gedropt door de juiste ASP-reden.

Bijvoorbeeld, ACL Drop, Firewall en Scanning bedreigingen allen overwegen het tarief van pakketten die door acl-drop worden gelaten vallen. Voltooi deze stappen om deze bedreigingen gelijktijdig teweeg te brengen:

1. Maak een ACL op de buiteninterface van de ASA die expliciet alle TCP-pakketten laat vallen die naar een doelserver binnen de ASA worden verzonden (10.11.11.11):

```
access-list outside_in extended line 1 deny tcp any host 10.11.11.11
access-list outside_in extended permit ip any any
access-group outside_in in interface outside
```

2. Van een aanvaller aan de buitenkant van de ASA (10.10.10.10), gebruik nmap om een TCP SYN-scan uit te voeren tegen elke poort op de doelserver:

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

> **Opmerking**: T5 configureert nmap om de scan zo snel mogelijk uit te voeren. Gebaseerd op de middelen van de aanvaller PC, is dit nog niet snel genoeg om sommige van de standaardtarieven teweeg te brengen. Als dit het geval is, verlaag dan gewoon de ingestelde tarieven voor de dreiging die u wilt zien. Als u de ARI en BRI op 0 instelt, veroorzaakt de Basic Threat Detection altijd de bedreiging, ongeacht de snelheid.

---

3. Bericht dat de BasisBedreigingen voor ACL Drop, Firewall, en het Scannen bedreigingen worden gedetecteerd:

```
%ASA-1-733100: [ Scanning] drop rate-1 exceeded. Current burst rate is 19 per second,
 max configured rate is 10; Current average rate is 9 per second,
 max configured rate is 5; Cumulative total count is 5538
%ASA-1-733100: [ ACL drop] drop rate-1 exceeded. Current burst rate is 19 per second,
 max configured rate is 0; Current average rate is 2 per second,
 max configured rate is 0; Cumulative total count is 1472
%ASA-1-733100: [ Firewall] drop rate-1 exceeded. Current burst rate is 18 per second,
 max configured rate is 0; Current average rate is 2 per second,
 max configured rate is 0; Cumulative total count is 1483
```

> **Opmerking**: in dit voorbeeld zijn de ACL-drop en de firewall ARI's en BRI's ingesteld op 0, zodat ze altijd een bedreiging veroorzaken. Dit is waarom de maximaal ingestelde snelheden worden weergegeven als 0.

Geavanceerde bedreigingen - TCP-onderschepping

1. Maak een ACL op de buiteninterface die alle TCP-pakketten toestaat die naar een doelserver binnen

de ASA (10.11.11.11) worden verzonden:

```
access-list outside_in extended line 1 permit tcp any host 10.11.11.11
access-group outside_in in interface outside
```

2. Als de doelserver niet echt bestaat, of als het de verbindingspogingen van de aanvaller terugstelt, vorm een valse ARP ingang op ASA om het aanvalsverkeer uit de binneninterface te zwarte gaten:

```
arp inside 10.11.11.11 dead.dead.dead
```

3. Maak een eenvoudig TCP-onderscheppingsbeleid op de ASA:

```
access-list tcp extended permit tcp any any
class-map tcp
  match access-list tcp
policy-map global_policy
  class tcp
    set connection conn-max 2
service-policy global_policy global
```

Van een aanvaller aan de buitenkant van de ASA (10.10.10.10), gebruik nmap om een TCP SYN-scan uit te voeren tegen elke poort op de doelserver:

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

Let op dat Threat Detection de beveiligde server bijhoudt:

<#root>

```
ciscoasa(config)#
```

show threat-detection statistics top tcp-intercept

```
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs

--------------------------------------------------------------------------------
1    10.11.11.11:18589 outside 0 0 1 10.10.10.10 (36 secs ago)
2    10.11.11.11:47724 outside 0 0 1 10.10.10.10 (36 secs ago)
3    10.11.11.11:46126 outside 0 0 1  Last: 10.10.10.10 (6 secs ago)
4    10.11.11.11:3695 outside 0 0 1  Last: 10.10.10.10 (6 secs ago)
```

Bedreiging scannen

1. Maak een ACL op de buiteninterface die alle TCP-pakketten toestaat die naar een doelserver binnen de ASA (10.11.11.11) worden verzonden:

```
access-list outside_in extended line 1 permit tcp any host 10.11.11.11
access-group outside_in in interface outside
```

Opmerking: om bedreigingsdetectie bij scannen te kunnen volgen op het doel en de aanvaller IP's, moet het verkeer via de ASA zijn toegestaan.

2. Als de doelserver niet echt bestaat, of als het de verbindingspogingen van de aanvaller terugstelt, vorm een valse ARP ingang op ASA om het aanvalsverkeer uit de binneninterface te zwarte gaten:

```
arp inside 10.11.11.11 dead.dead.dead
```

Opmerking: verbindingen die door de doelserver worden hersteld, worden niet meegeteld als deel van de bedreiging.

3. Van een aanvaller aan de buitenkant van de ASA (10.10.10.10), gebruik nmap om een TCP SYN-scan uit te voeren tegen elke poort op de doelserver:

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

Opmerking: T5 configureert nmap om de scan zo snel mogelijk uit te voeren. Gebaseerd op de middelen van de aanvaller PC, is dit nog niet snel genoeg om sommige van de standaardtarieven teweeg te brengen. Als dit het geval is, verlaag dan gewoon de ingestelde tarieven voor de dreiging die u wilt zien. Als u de ARI en BRI op 0 instelt, veroorzaakt de Basic Threat Detection altijd de bedreiging, ongeacht de snelheid.

4. Merk op dat een Scanning-dreiging wordt gedetecteerd, het IP van de aanvaller wordt bijgehouden en de aanvaller wordt gegijzeld:

```
%ASA-1-733100: [ Scanning] drop rate-1 exceeded. Current burst rate is 17 per second,
max configured rate is 10; Current average rate is 0 per second,
 max configured rate is 5; Cumulative total count is 404
%ASA-4-733101: Host 10.10.10.10 is attacking. Current burst rate is 17 per second,
 max configured rate is 10; Current average rate is 0 per second,
 max configured rate is 5; Cumulative total count is 700
%ASA-4-733102: Threat-detection adds host 10.10.10.10 to shun list
```

Gerelateerde informatie

- **ASA-configuratiehandleiding**
- **ASA Command Reference**
- **Cisco Secure Firewall ASA Series systeemmeldingen**
- **Cisco technische ondersteuning 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.