Shunning/blokkering van IPS voor ASA/PIX/IOS routerconfiguratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u het draaien op een PIX/ASA/Cisco IOS router met de hulp van Cisco IPS kunt configureren. ARC, de blokkerende toepassing op de sensor, start en stop blokken op routers, Cisco 5000 RSM en Catalyst 6500 Series switches, PIX Firewalls, FWSM en ASA. ARC geeft een blok of herkenning uit aan het beheerde apparaat voor het kwaadaardige IP-adres. BOOG stuurt hetzelfde blok naar alle apparaten die de sensor beheert. Als een primaire blokkeringssensor is ingesteld, wordt het blok naar dit apparaat doorgestuurd en van dit apparaat afgegeven. ARC controleert de tijd voor het blok en verwijdert het blok nadat de tijd is verstreken.

Wanneer u IPS 5.1 gebruikt, moet u bijzonder voorzichtig zijn bij het verzenden naar firewalls in meerdere context-modus omdat er geen VLAN-informatie met het shun-verzoek wordt verzonden.

> Opmerking: De blokkering wordt niet ondersteund in de beheercontext van een meervoudige context-FWSM.

Er zijn drie typen blokken:

- Host block-Blokleert al verkeer vanaf een bepaald IP-adres.
- Koppel-blokkeert verkeer van een bepaald bron-IP-adres naar een bepaald bestemming IP-adres en een doelpoort. Meervoudige verbindingsblokken van het zelfde bron IP adres aan of een verschillend bestemming IP adres of de bestemmingspoort veranderen automatisch het blok van een verbindingsblok aan een host blok.Opmerking: Aansluitblokken worden niet ondersteund door beveiligingsapparaten. Beveiligingsapparaten ondersteunen alleen hostblokken met optionele poort- en protocolinformatie.
- Netwerkblokkering - blokkeert al het verkeer vanaf een bepaald netwerk. U kunt host- en

verbindingsblokken handmatig of automatisch openen wanneer een handtekening is geactiveerd. U kunt netwerkblokken alleen handmatig openen.

Voor automatische blokken moet u Blok van de Aanvraag of Blok van de Aanvraag van de Aanvraag als de gebeurtenis actie voor bepaalde handtekeningen kiezen, zodat SensorApp een blokverzoek naar BOC verstuurt wanneer de handtekening wordt geactiveerd. Zodra ARC het blokverzoek van SensorApp ontvangt, werkt het de apparaatconfiguraties bij om de host of verbinding te blokkeren. Zie Handelingen toewijzen aan handtekeningen, pagina 5-22 voor meer informatie over de procedure om de groepshost-aanvraag toe te voegen of blokverbinding aanvragen aan de handtekening aan te vragen. Raadpleeg Het configureren van Event Action Overrides, pagina 7-15 voor meer informatie over de procedure voor het configureren van overgangen die de handelingen voor blokkering van host aanvragen of blokkering van verbindingen aanvragen toevoegen aan waarschuwingen over specifieke risicobeoordelingen.

Op Cisco routers en Catalyst 6500 Series switches maakt ARC blokken door ACL's of VACL's toe te passen. ACL's en VACL's passen filters op interfaces toe, die richting en VLAN's omvatten, respectievelijk om verkeer toe te staan of te ontkennen. . De PIX Firewall, FWSM, en ASA gebruiken geen ACL's of VACL's. De ingebouwde **shun** en **geen geweer** worden gebruikt.

Deze informatie is vereist voor de configuratie van BOOG:

- Login user ID (indien het apparaat met AAA is ingesteld)
- Aanmelden wachtwoord
- Wachtwoord inschakelen, wat niet nodig is als de gebruiker privileges heeft ingeschakeld
- Te beheren interfaces, bijvoorbeeld ethernet0, VLAN100
- Alle bestaande ACL- of VACL-informatie die u wilt toepassen aan het begin (Voorblokkerend ACL of VACL) of eind (Post-Blok ACL of VACL) van de ACL of VACL die wordt gecreëerd. Dit is niet van toepassing op een PIX-firewall, FWSM of ASA omdat ze geen ACL's of VACL's gebruiken om te blokkeren.
- Of u Telnet of SSH gebruikt om met het apparaat te communiceren
- IP-adressen (host of bereik van hosts) die u nooit geblokkeerd wilt hebben
- Hoe lang je wilt dat de blokken blijven bestaan

Voorwaarden

Vereisten

Voordat u ARC configureren voor het blokkeren of beperken van snelheden, moet u deze taken voltooien:

- Analyseer uw netwerktopologie om te begrijpen welke apparaten door welke sensor moeten worden geblokkeerd, en welke adressen nooit zouden moeten worden geblokkeerd.
- Verzamel de gebruikersnamen, de wachtwoorden van het apparaat, laat wachtwoorden, en de types van verbindingen (telnet of SSH) toe nodig om aan elk apparaat in te loggen.
- Ken de interfacenamen op de apparaten.
- Weet u de namen van de Pre-Block ACL of VACL en de Post-Block ACL of VACL indien nodig.
- Begrijp welke interfaces moeten en mogen niet worden geblokkeerd en in welke richting (in of uit).

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Inbraakpreventiesysteem 5.1 en hoger.

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.

> Opmerking: Standaard wordt ARC ingesteld voor een limiet van 250 blokitems. Raadpleeg Ondersteunde apparaten voor meer informatie over de lijst met blokkerende apparaten die worden ondersteund door ARC.

Conventies

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

Achtergrondinformatie

Gebruik de blokkeerpagina om de basisinstellingen te configureren die nodig zijn voor het blokkeren en beperken van snelheden.

BOOG controleert blokkerende en snelheidsbeperkende maatregelen op beheerde apparaten.

Je moet je sensor aanpassen om hosts en netwerken te identificeren die nooit geblokkeerd zouden moeten worden. Het verkeer van een betrouwbaar apparaat kan een handtekening ontslaan. Als deze handtekening is ingesteld om de aanvaller te blokkeren, kan het legitieme netwerkverkeer worden beïnvloed. Het IP-adres van het apparaat kan in de lijst Never Block worden opgenomen om dit scenario te voorkomen.

Een netmask die in een "Never Block entry" wordt gespecificeerd, wordt op het "Never Block adres" toegepast. Als geen netmask wordt gespecificeerd, wordt een standaard/32 masker toegepast.

> Opmerking: Standaard is de sensor niet toegestaan om een blok voor zijn eigen IP-adres uit te geven omdat dit de communicatie tussen de sensor en het blokkeerapparaat verstoort. Maar deze optie is configureerbaar door de gebruiker.

Als ARC is ingesteld voor het beheren van een blokkerend apparaat, mogen de schaduwen van het blokkerende apparaat en ACL's/VACL's die worden gebruikt voor blokkering niet handmatig worden gewijzigd. Dit kan leiden tot een verstoring van de ARC-service en kan ertoe leiden dat in de toekomst geen blokkeringen worden uitgegeven.

> Opmerking: Standaard wordt alleen blokkering ondersteund op Cisco IOS-apparaten. U kunt het blokkeren standaard omzeilen als u snelheidsbeperking of blokkering plus snelheidsbeperking kiest.

Om blokken uit te geven of te wijzigen, moet de IPS-gebruiker de beheerder of de operator een rol hebben.

Configureer de sensor om Cisco-routers te beheren

In deze sectie wordt beschreven hoe u de sensor kunt configureren voor het beheer van Cisco-routers. Het bevat deze onderwerpen:

- Gebruikersprofielen configureren
- Routers en ACL's
- Cisco-routers configureren met CLI

Gebruikersprofielen configureren

De sensor beheert de andere apparaten met de opdracht **gebruikersprofielen** *profile_name* om gebruikersprofielen in te stellen. De gebruikersprofielen bevatten de gebruikersnaam, het wachtwoord en geven wachtwoordinformatie weer. Bijvoorbeeld, routers die alle dezelfde wachtwoorden en gebruikersnamen delen kunnen onder één gebruikersprofiel staan.

> Opmerking: U **moet** een gebruikersprofiel maken voordat u het blokkerende apparaat configureren.

Voltooi deze stappen om gebruikersprofielen in te stellen:

1. Meld u aan bij de CLI met een account met Administrator-rechten.
2. Geef de toegangsmodus voor het netwerk op.
   ```
   sensor#configure terminal
   sensor(config)#service network-access
   sensor(config-net)#
   ```
3. De naam van het gebruikersprofiel maken.
   ```
   sensor(config-net)#user-profiles PROFILE1
   ```
4. Typ de gebruikersnaam voor dat gebruikersprofiel.
   ```
   sensor(config-net-use)#username username
   ```
5. Specificeer het wachtwoord voor de gebruiker.
   ```
   sensor(config-net-use)# password
   Enter password[]: ********
   Re-enter password ********
   ```
6. Specificeer het wachtwoord voor het inschakelen van de gebruiker.
   ```
   sensor(config-net-use)# enable-password
   Enter enable-password[]: ********
   Re-enter enable-password ********
   ```
7. Controleer de instellingen.
   ```
   sensor(config-net-use)#show settings
      profile-name: PROFILE1
      -----------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: jsmith default:
      -----------------------------------------------
   ```

```
sensor(config-net-use)#
```

8. Submode voor netwerktoegang afsluiten.

```
sensor(config-net-use)#exit
sensor(config-net)#exit
Apply Changes:?[yes]:
```

9. Druk op **Voer** in om de wijzigingen toe te passen of geef een nr in om ze weg te gooien.

Routers en ACL's

Wanneer ARC is ingesteld met een blokkerend apparaat dat ACL's gebruikt, bestaan de ACL's op deze manier:

1. Een vergunningslijn met het IP-adres van de sensor of, indien gespecificeerd, het NAT-adres van de sensorOpmerking: Als u toestaat dat de sensor wordt geblokkeerd, verschijnt deze lijn niet in ACL.
2. Voorblokkeerbaar ACL (indien gespecificeerd): Deze ACL moet al op het apparaat bestaan.Opmerking: BOOG leest de lijnen in de vooraf ingestelde ACL en kopieert deze lijnen naar het begin van het blok ACL.
3. Alle actieve blokken
4. **Post-Block ACL** of **sta toe om**:**Post-Blok ACL** (indien gespecificeerd):Deze ACL moet al op het apparaat bestaan.Opmerking: BOOG leest de lijnen in ACL en kopieert deze lijnen naar het eind van ACL.Opmerking: Zorg ervoor dat de laatste regel in ACL om het even welke lijn is toegestaan als u wilt dat alle niet-afgesloten pakketten worden toegestaan.**Laat elke** (niet gebruikte) toegangsweg **ip** toe als een Post-Block ACL is gespecificeerd)

   Opmerking: De ACL's die BOC maakt zouden nooit door u of een ander systeem moeten worden aangepast. Deze ACL's zijn tijdelijk en nieuwe ACL's worden constant gemaakt door de sensor. De enige wijzigingen die u kunt maken zijn aan de pre- en Post-Block ACL's.

Als u de ACL's (vooraf blokkeren of achteraf) moet wijzigen, voltooit u deze stappen:

1. Afsluiten op de sensor.
2. Breng de wijzigingen aan in de configuratie van het apparaat.
3. Afsluitbaar op de sensor.

Wanneer blokkering is ingeschakeld, leest de sensor de nieuwe configuratie van het apparaat.

Opmerking: Een enkele sensor kan meerdere apparaten beheren, maar meerdere sensoren kunnen één apparaat niet besturen. Indien blokken die zijn afgegeven door meerdere sensoren bestemd zijn voor één blokkeringsvoorziening, moet een primaire blokkeringssensor in het ontwerp worden ingebouwd. Een primaire blokkeringssensor ontvangt blokkeringsverzoeken van meerdere sensoren en geeft alle blokkeringsverzoeken aan het blokkerende apparaat af.

U maakt en slaat Pre-Block en Post-Block ACL's op in uw routerconfiguratie. Deze ACL's moeten worden uitgebreid, IP-ACL's genoemd of genummerd. Zie uw routerdocumentatie voor meer informatie over het maken van ACL's.

Opmerking: ACLS vóór en na blokkering zijn niet van toepassing op snelheidsbeperking.

ACL's worden van boven naar beneden geëvalueerd en de eerste-match actie wordt ondernomen. Pre-Blok ACL kan een vergunning bevatten die voorrang zou hebben op ontkennen die uit een blok voortkwam.

De Post-Blok ACL wordt gebruikt om rekening te houden met om het even welke voorwaarden die niet door de Pre-Block ACL of blokken worden behandeld. Als u een bestaande ACL op de interface en in de richting die de blokken worden afgegeven hebt, kan ACL als Post-Blok ACL worden gebruikt. Als u geen Post-Blok ACL hebt, staan de sensorinsteken om het even welke aan het eind van nieuwe ACL toe.

Wanneer de sensor begint, leest hij de inhoud van de twee ACL's. Er wordt een derde ACL-schijf gemaakt met deze items:

- Een vergunningslijn voor het IP-adres van de sensor
- Kopieën van alle configuratielijnen van het Pre-Block ACL
- Een ontkenningslijn voor elk adres dat geblokkeerd is door de sensor
- Kopieën van alle configuratielijnen van het Post-Blok ACL

De sensor past de nieuwe ACL op de interface en richting toe die u aanwijst.

> Opmerking: Wanneer het nieuwe blok ACL op een interface van de router, in een bepaalde richting wordt toegepast, vervangt het om het even welke reeds bestaande ACL op die interface in die richting.

Cisco-routers configureren met CLI

Voltooi deze stappen om een sensor te configureren om een Cisco router te beheren om blokkering en snelheidsbeperking uit te voeren:

1. Meld u aan bij de CLI met een account met Administrator-rechten.
2. Typ de submodus voor netwerktoegang.
   ```
   sensor#configure terminal
   sensor(config)#service network-access
   sensor(config-net)#
   ```
3. Specificeer het IP-adres voor de router die door ARC beheerst is.
   ```
   sensor(config-net)#router-devices ip_address
   ```
4. Voer de naam van het logische apparaat in die u hebt gemaakt toen u het gebruikersprofiel hebt ingesteld.
   ```
   sensor(config-net-rou)#profile-name user_profile_name
   ```
   Opmerking: BOOG accepteert alles wat je ingeeft. Er wordt niet gecontroleerd of het gebruikersprofiel bestaat.
5. Specificeer de methode die gebruikt wordt om toegang tot de sensor te krijgen.
   ```
   sensor(config-net-rou)# communication {telnet | ssh-des | ssh-3des}
   ```

   Indien niet gespecificeerd, wordt SSH 3DES gebruikt.Opmerking: Als u DES of 3DES gebruikt, moet u de **ssh host-key ip_address** opdracht gebruiken om de SSH-toets van het apparaat te aanvaarden.
6. Specificeer het NAT-adres van de sensor.
   ```
   sensor(config-net-rou)#nat-address nat_address
   ```
   Opmerking: Dit verandert het IP adres in de eerste regel van ACL van het adres van de

sensor in het NAT adres. Het NAT-adres is het sensoradres, post-NAT, vertaald door een intermediair apparaat, dat zich tussen de sensor en het blokkeerapparaat bevindt.

7. Specificeer of de router blokkering, snelheidsbeperking of beide uitvoert.Opmerking: De standaardinstelling is het blokkeren. U hoeft de reactiemogelijkheden niet te configureren als u wilt dat de router alleen blokkering uitvoert.Alleen snelheidsbeperking
   ```
   sensor(config-net-rou)#response-capabilities rate-limit
   ```

   Zowel blokkering als snelheidsbeperking
   ```
   sensor(config-net-rou)#response-capabilities block|rate-limit
   ```

8. Specificeer de interfacenaam en -richting.
   ```
   sensor(config-net-rou)#block-interfaces interface_name {in | out}
   ```

   Opmerking: De naam van de interface moet een afkorting zijn die de router herkent wanneer gebruikt na de opdracht **interface**.
9. (Optioneel) Voeg de voornaam van de ACL toe (alleen blokkeren).
   ```
   sensor(config-net-rou-blo)#pre-acl-name pre_acl_name
   ```
10. (Optioneel) Voeg de post-ACL naam toe (alleen blokkerend).
    ```
    sensor(config-net-rou-blo)#post-acl-name post_acl_name
    ```
11. Controleer de instellingen.
    ```
    sensor(config-net-rou-blo)#exit

    sensor(config-net-rou)#show settings

       ip-address: 10.89.127.97
       ----------------------------------------------
          communication: ssh-3des default: ssh-3des
          nat-address: 19.89.149.219 default: 0.0.0.0
          profile-name: PROFILE1
          block-interfaces (min: 0, max: 100, current: 1)
          ----------------------------------------------
             interface-name: GigabitEthernet0/1
             direction: in
             ----------------------------------------------
                pre-acl-name: <defaulted>
                post-acl-name: <defaulted>
             ----------------------------------------------
          ----------------------------------------------
          response-capabilities: block|rate-limit default: block
       ----------------------------------------------
    sensor(config-net-rou)#
    ```
12. Submode voor netwerktoegang afsluiten.
    ```
    sensor(config-net-rou)#exit
    sensor(config-net)#exit
    sensor(config)#exit
    Apply Changes:?[yes]:
    ```
13. Druk op **ENTER** om de wijzigingen toe te passen of **nee** in te voeren om ze weg te gooien.

Configuratie van de sensor om Cisco Firewalls te beheren

Voltooi deze stappen om de sensor te configureren om Cisco-firewalls te beheren:

1. Meld u aan bij de CLI met een account met Administrator-rechten.
2. Typ de submodus voor netwerktoegang.
   ```
   sensor#configure terminal
   ```

```
sensor(config)#service network-access
sensor(config-net)#
```

3. Specificeer het IP-adres voor de firewall die door ARC wordt gecontroleerd.
   ```
   sensor(config-net)#firewall-devices ip_address
   ```
4. Voer de naam van het gebruikersprofiel in die u hebt gemaakt toen u het gebruikersprofiel hebt ingesteld.
   ```
   sensor(config-net-fir)#profile-name user_profile_name
   ```
   Opmerking: ARC accepteert alles wat u typt. Het controleert niet of het logische hulpmiddel bestaat.
5. Specificeer de methode die gebruikt wordt om toegang tot de sensor te krijgen.
   ```
   sensor(config-net-fir)#communication {telnet | ssh-des | ssh-3des}
   ```

   Indien niet gespecificeerd, wordt SSH 3DES gebruikt.Opmerking: Als u DES of 3DES gebruikt, moet u de **ssh host-key ip_address** opdracht gebruiken om de toets te accepteren of kan ARC geen verbinding maken met het apparaat.
6. Specificeer het NAT-adres van de sensor.
   ```
   sensor(config-net-fir)#nat-address nat_address
   ```
   Opmerking: Dit verandert het IP adres in de eerste regel van ACL van het IP adres van de sensor in het NAT adres. Het NAT-adres is het sensoradres, post-NAT, vertaald door een intermediair apparaat, dat zich tussen de sensor en het blokkeerapparaat bevindt.
7. Submode voor netwerktoegang afsluiten.
   ```
   sensor(config-net-fir)#exit
   sensor(config-net)#exit
   sensor(config)#exit
   Apply Changes:?[yes]:
   ```
8. Druk op **Voer** in om de wijzigingen toe te passen of **ga** het **niet** in om ze weg te gooien.

Blok met SHUN in PIX/ASA

De **shun** commando blokkeert verbindingen van een aanvaller. Pakketten die overeenkomen met de waarden in de opdracht, worden geworpen en geregistreerd totdat de blokkeringsfunctie is verwijderd. De **shun** wordt toegepast ongeacht of een verbinding met het opgegeven host-adres momenteel actief is.

Als u het doeladres, de bron- en de doelpoorten en het protocol specificeert, enkt u de straal aan verbindingen die overeenkomen met deze parameters. U kunt slechts één **shun** opdracht voor elk bron IP-adres hebben.

Omdat de opdracht Shun wordt gebruikt om aanvallen dynamisch te blokkeren, wordt dit niet weergegeven in de configuratie van het beveiligingsapparaat.

Wanneer een interface wordt verwijderd, worden alle schaduwen die op die interface zijn aangesloten ook verwijderd.

Dit voorbeeld laat zien dat de beledigende gastheer (10.1.1.27) een verbinding met het slachtoffer (10.2.2.89) aan TCP maakt. De aansluiting in de tabel met verbindingen van het beveiligingsapparaat luidt als volgt:

```
TCP outside:10.1.1.27/555 inside:10.2.2.89/666
```

Om verbindingen van een aanvallende gastheer te blokkeren, gebruik het **bevel** van de **shun** in bevoorrechte EXEC wijze. Pas de **shun**-opdracht met deze opties toe:

```
hostname#shun 10.1.1.27 10.2.2.89 555 666 tcp
```

De opdracht verwijdert de aansluiting uit de verbindingstabel van het security apparaat en voorkomt ook dat pakketten van 10.1.1.27:55 tot 10.2.2.89:66 (TCP) door het security apparaat gaan.

Gerelateerde informatie

- De sensor configureren om Catalyst 6500 Series-switches en Cisco 7600 Series routers te beheren
- Technische ondersteuning en documentatie – Cisco Systems