Herunterfahren/Sperren von IPS für ASA/PIX/IOS-Router - Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie mithilfe von Cisco IPS das Herunterfahren auf einem PIX/ASA/Cisco IOS-Router konfigurieren. ARC, die Blockierungsanwendung auf dem Sensor, startet und stoppt Blöcke auf Routern, Switches der Serien Cisco 5000 RSM und Catalyst 6500, PIX-Firewalls, FWSM und ASA. ARC gibt für die schädliche IP-Adresse einen Block aus oder schaltet das verwaltete Gerät aus. ARC sendet denselben Block an alle Geräte, die der Sensor verwaltet. Wenn ein primärer Blockierungssensor konfiguriert ist, wird der Block an dieses Gerät weitergeleitet und von diesem ausgegeben. ARC überwacht die Zeit für den Block und entfernt den Block, nachdem die Zeit abgelaufen ist.

Wenn Sie IPS 5.1 verwenden, müssen Sie besonders vorsichtig sein, wenn Sie Firewalls im Multiple-Context-Modus meiden, da bei der Shun-Anforderung keine VLAN-Informationen gesendet werden.

> **Hinweis**: Blockierung wird im Admin-Kontext eines FWSM mit mehreren Kontexten nicht unterstützt.

Es gibt drei Blocktypen:

- Host Block (Hostblock): Blockiert den gesamten Datenverkehr von einer bestimmten IP-Adresse.
- Connection Block (Verbindungsblock): Blockiert den Datenverkehr von einer IP-Quelladresse zu einer bestimmten Ziel-IP-Adresse und einem Zielport. Mehrere Verbindungsblöcke von derselben Quell-IP-Adresse zu einer anderen Ziel-IP-Adresse oder einem anderen Ziel-Port schalten den Block automatisch von einem Verbindungsblock zu einem Host-Block

um.**Hinweis**: Verbindungsblöcke werden von Sicherheitsgeräten nicht unterstützt. Security Appliances unterstützen nur Hostblöcke mit optionalen Port- und Protokollinformationen.
- Netzwerkblock: Blockiert den gesamten Datenverkehr aus einem bestimmten Netzwerk. Sie können Host- und Verbindungsblöcke manuell oder automatisch initiieren, wenn eine Signatur ausgelöst wird. Sie können Netzwerkblöcke nur manuell initiieren.

Für automatische Blöcke müssen Sie als Ereignisaktion für bestimmte Signaturen Request Block Host (Host für Sperrblock anfordern) oder Request Block Connection (Verbindung anfordern) auswählen, sodass SensorApp eine Blockanforderung an ARC sendet, wenn die Signatur ausgelöst wird. Sobald ARC die Blockanforderung von SensorApp erhält, aktualisiert es die Gerätekonfigurationen, um den Host oder die Verbindung zu blockieren. Weitere Informationen zum Hinzufügen der Ereignisaktionen zum Request Block Host oder Request Block Connection zur Signatur finden Sie auf Seite 5-22 unter Zuweisen von Aktionen zu Signaturen. Weitere Informationen zum Verfahren für die Konfiguration von Überschreibungen, die die Ereignishandlungs-Host- oder Request Block Connection-Ereignisaktionen zu Alarmen mit spezifischen Risikobewertungen hinzufügen, finden Sie unter Configuring Event Action Overrides, Seite 7-15.

Auf Cisco Routern und Catalyst Switches der Serie 6500 erstellt ARC Blöcke durch Anwenden von ACLs oder VACLs. ACLs und VACLs wenden Filter auf Schnittstellen an (einschließlich Richtung), bzw. auf VLANs, um Datenverkehr zuzulassen oder abzulehnen. . Die PIX Firewall, FWSM und ASA verwenden keine ACLs oder VACLs. Der integrierte Befehl **shun** und **no shun** werden verwendet.

Diese Informationen sind für die Konfiguration von ARC erforderlich:

- Anmelde-Benutzer-ID, wenn das Gerät mit AAA konfiguriert ist
- Anmeldungs-Passwort
- Kennwort aktivieren, das nicht benötigt wird, wenn der Benutzer über Berechtigungen verfügt
- Zu verwaltende Schnittstellen, z. B. Ethernet0, VLAN100
- Alle vorhandenen ACL- oder VACL-Informationen, die Sie verwenden möchten, werden am Anfang (Pre-Block ACL oder VACL) oder Ende (Post-Block ACL oder VACL) der erstellten ACL oder VACL angewendet. Dies gilt nicht für eine PIX-Firewall, FWSM oder ASA, da sie keine ACLs oder VACLs zum Blockieren verwenden.
- Ob Sie Telnet oder SSH für die Kommunikation mit dem Gerät verwenden
- IP-Adressen (Host oder Hosts), die Sie niemals blockieren möchten
- Dauer der Blöcke

Voraussetzungen

Anforderungen

Bevor Sie ARC für die Blockierung oder die Ratenbegrenzung konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

- Analysieren Sie die Netzwerktopologie, um zu ermitteln, welche Geräte von welchem Sensor blockiert werden sollten und welche Adressen niemals blockiert werden sollten.
- Sammeln Sie die Benutzernamen, Gerätekennwörter, Aktivierungskennwörter und Verbindungstypen (Telnet oder SSH), die für die Anmeldung bei jedem Gerät erforderlich

sind.
- Machen Sie sich mit den Schnittstellennamen auf den Geräten vertraut.
- Machen Sie sich mit den Namen der Pre-Block ACL oder VACL und der Post-Block ACL bzw. VACL vertraut.
- Informieren Sie sich darüber, welche Schnittstellen blockiert werden sollen und in welche Richtung (ein- oder ausgehend).

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco Intrusion Prevention System 5.1 und höher.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

> **Hinweis**: ARC ist standardmäßig für eine Beschränkung auf 250 Blockeinträge konfiguriert. Unter Unterstützte Geräte finden Sie weitere Informationen zur Liste der von ARC unterstützten blockierenden Geräte.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Auf der Seite Blockierung können Sie die grundlegenden Einstellungen konfigurieren, die zum Aktivieren der Blockierung und der Ratenbegrenzung erforderlich sind.

ARC kontrolliert die Blockierung und Ratenbegrenzung von Aktionen auf verwalteten Geräten.

Sie müssen den Sensor anpassen, um Hosts und Netzwerke zu identifizieren, die niemals blockiert werden sollten. Der Datenverkehr eines vertrauenswürdigen Geräts kann eine Signatur auslösen. Wenn diese Signatur so konfiguriert ist, dass sie den Angreifer blockiert, kann der legitime Netzwerkverkehr beeinträchtigt werden. Die IP-Adresse des Geräts kann in der Liste Nie blockierter Geräte aufgeführt werden, um dieses Szenario zu verhindern.

Eine in einem Eintrag Nie blockierende Netzmaske wird auf die Adresse Nie blockieren angewendet. Wenn keine Netzmaske angegeben ist, wird eine Standardmaske /32 angewendet.

> **Hinweis**: Standardmäßig ist es dem Sensor nicht gestattet, einen Block für seine eigene IP-Adresse auszugeben, da dies die Kommunikation zwischen dem Sensor und dem Blockierungsgerät beeinträchtigt. Diese Option kann jedoch vom Benutzer konfiguriert werden.

Nachdem ARC für die Verwaltung eines Blockierungsgeräts konfiguriert wurde, sollten die Shuns und ACLs/VACLs des blockierenden Geräts, die für die Blockierung verwendet werden, nicht manuell geändert werden. Dies kann zu einer Unterbrechung des ARC-Services führen und dazu führen, dass künftige Blöcke nicht ausgegeben werden.

> **Hinweis**: Standardmäßig wird nur die Blockierung auf Cisco IOS-Geräten unterstützt. Sie können den Blockierungsstandard überschreiben, wenn Sie die Ratenbeschränkung oder Blockierung plus Ratenbegrenzung wählen.

Um Blöcke auszugeben oder zu ändern, muss der IPS-Benutzer über die Rolle Administrator oder Operator verfügen.

Konfigurieren des Sensors zum Verwalten von Cisco Routern

In diesem Abschnitt wird beschrieben, wie Sie den Sensor für die Verwaltung von Cisco Routern konfigurieren. Folgende Themen werden behandelt:

- Benutzerprofile konfigurieren
- Router und ACLs
- Konfigurieren von Cisco Routern mithilfe der CLI

Benutzerprofile konfigurieren

Der Sensor verwaltet die anderen Geräte mit dem Befehl **user-profiles** *profile_name*, um Benutzerprofile einzurichten. Die Benutzerprofile enthalten die Benutzer-ID, das Kennwort und die Kennwortinformationen für das Aktivieren. Router, die alle dieselben Kennwörter und Benutzernamen verwenden, können beispielsweise unter einem Benutzerprofil gespeichert werden.

> **Hinweis**: Sie **müssen** ein Benutzerprofil erstellen, bevor Sie das blockierende Gerät konfigurieren.

Gehen Sie wie folgt vor, um Benutzerprofile einzurichten:

1. Melden Sie sich bei der CLI mit einem Konto mit Administratorrechten an.
2. Wechseln Sie in den Netzwerkzugriffsmodus.
   ```
   sensor#configure terminal
   sensor(config)#service network-access
   sensor(config-net)#
   ```
3. Erstellen Sie den Benutzerprofilnamen.
   ```
   sensor(config-net)#user-profiles PROFILE1
   ```
4. Geben Sie den Benutzernamen für dieses Benutzerprofil ein.
   ```
   sensor(config-net-use)#username username
   ```
5. Geben Sie das Kennwort für den Benutzer an.
   ```
   sensor(config-net-use)# password
   Enter password[]: ********
   Re-enter password ********
   ```
6. Geben Sie das enable-Kennwort für den Benutzer an.

```
sensor(config-net-use)# enable-password
Enter enable-password[]: ********
Re-enter enable-password ********
```

7. Überprüfen Sie die Einstellungen.
```
sensor(config-net-use)#show settings
   profile-name: PROFILE1
   -----------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: jsmith default:
   -----------------------------------------------
sensor(config-net-use)#
```
8. Beenden Sie den Submodus für den Netzwerkzugriff.
```
sensor(config-net-use)#exit
sensor(config-net)#exit
Apply Changes:?[yes]:
```
9. Drücken Sie die **Eingabetaste**, um die Änderungen anzuwenden, oder geben Sie no ein, um sie zu verwerfen.

Router und ACLs

Wenn ARC mit einem Blockierungsgerät konfiguriert wird, das ACLs verwendet, werden die ACLs folgendermaßen zusammengesetzt:

1. Eine Genehmigungsleitung mit der Sensor-IP-Adresse oder, falls angegeben, der NAT-Adresse des Sensors**Hinweis**: Wenn Sie zulassen, dass der Sensor blockiert wird, wird diese Zeile nicht in der ACL angezeigt.
2. ACL vor der Blockierung (falls angegeben): Diese ACL muss bereits auf dem Gerät vorhanden sein.**Hinweis**: ARC liest die Zeilen in der vorkonfigurierten ACL und kopiert diese Zeilen in den Anfang der Block-ACL.
3. Alle aktiven Blöcke
4. Entweder **Post-Block-ACL** oder **permit ip any**:**ACL nach dem Blockieren** (falls angegeben):Diese ACL muss bereits auf dem Gerät vorhanden sein.**Hinweis**: ARC liest die Zeilen in der ACL und kopiert diese Zeilen bis zum Ende der ACL.**Hinweis**: Vergewissern Sie sich, dass die letzte Zeile in der ACL "permit ip any any" lautet, wenn Sie möchten, dass alle nicht übereinstimmenden Pakete zugelassen werden.**permit ip any any** (wird nicht verwendet, wenn eine Post-Block-ACL angegeben ist)

   Hinweis: Die von ARC erstellten ACLs sollten niemals von Ihnen oder einem anderen System geändert werden. Diese Zugriffskontrolllisten sind temporär, und der Sensor erstellt ständig neue Zugriffskontrolllisten. Sie können nur die Vor- und Nachblockzugriffskontrolllisten ändern.

Wenn Sie die Zugriffskontrollliste vor oder nach dem Block ändern müssen, gehen Sie wie folgt vor:

1. Deaktivieren Sie die Blockierung auf dem Sensor.
2. Nehmen Sie die Änderungen an der Konfiguration des Geräts vor.
3. Aktivieren Sie die Blockierung auf dem Sensor wieder.

Wenn die Blockierung erneut aktiviert wird, liest der Sensor die neue Gerätekonfiguration.

> **Hinweis**: Ein einzelner Sensor kann mehrere Geräte verwalten, aber mehrere Sensoren können nicht ein Gerät verwalten. Falls Blöcke von mehreren Sensoren für ein einziges Blockierungsgerät bestimmt sind, muss ein primärer Blockierungssensor in das Design integriert werden. Ein primärer Blockierungssensor empfängt Blockierungsanfragen von mehreren Sensoren und leitet alle Blockierungsanfragen an das Blockierungsgerät weiter.

Sie erstellen und speichern Pre-Block- und Post-Block-ACLs in der Router-Konfiguration. Diese ACLs müssen erweiterte IP-ACLs sein, die entweder benannt oder nummeriert sind. Weitere Informationen zum Erstellen von ACLs finden Sie in der Router-Dokumentation.

> **Hinweis**: Vor- und nach dem Block-Angriff genutzte ACLS gelten nicht für die Ratenbegrenzung.

Die ACLs werden von oben nach unten ausgewertet, und die erste Übereinstimmung wird erzielt. Die Pre-Block ACL kann eine Berechtigung enthalten, die Vorrang vor einer Leugnung hat, die aus einem Block resultiert.

Die Post-Block-ACL wird für alle Bedingungen verwendet, die nicht von der Pre-Block ACL oder den Blöcken behandelt werden. Wenn auf der Schnittstelle und in der Richtung, in der die Blöcke ausgegeben werden, eine vorhandene ACL vorhanden ist, kann diese als Post-Block-ACL verwendet werden. Wenn Sie keine Post-Block-ACL haben, erlauben die Sensoreinsätze "ip any" am Ende der neuen ACL.

Beim Start des Sensors liest er den Inhalt der beiden ACLs. Es wird eine dritte ACL mit folgenden Einträgen erstellt:

- Eine Genehmigungszeile für die IP-Adresse des Sensors
- Kopien aller Konfigurationslinien der Pre-Block ACL
- Eine Ablehnungszeile für jede vom Sensor blockierte Adresse
- Kopien aller Konfigurationslinien der Post-Block-ACL

Der Sensor wendet die neue ACL auf die von Ihnen festgelegte Schnittstelle und Richtung an.

> **Hinweis**: Wenn die neue Block-ACL auf eine Schnittstelle des Routers in einer bestimmten Richtung angewendet wird, ersetzt sie alle vorhandenen ACLs an dieser Schnittstelle in diese Richtung.

Konfigurieren von Cisco Routern mithilfe der CLI

Gehen Sie wie folgt vor, um einen Sensor für die Verwaltung eines Cisco Routers zu konfigurieren, der Blockierung und Ratenbegrenzung durchführt:

1. Melden Sie sich bei der CLI mit einem Konto mit Administratorrechten an.
2. Wechseln Sie in den Submodus für den Netzwerkzugriff.
   ```
   sensor#configure terminal
   sensor(config)#service network-access
   sensor(config-net)#
   ```
3. Geben Sie die IP-Adresse für den Router an, der von ARC gesteuert wird.
   ```
   sensor(config-net)#router-devices ip_address
   ```
4. Geben Sie den Namen des logischen Geräts ein, den Sie bei der Konfiguration des

Benutzerprofils erstellt haben.
`sensor(config-net-rou)#`**`profile-name`** *`user_profile_name`*
Hinweis: ARC akzeptiert alle von Ihnen eingegebenen Daten. Es wird nicht überprüft, ob das Benutzerprofil vorhanden ist.

5. Geben Sie die Methode für den Zugriff auf den Sensor an.
`sensor(config-net-rou)#` **`communication {telnet | ssh-des | ssh-3des}`**

   Bei nicht spezifizierter Variante wird SSH 3DES verwendet.**Hinweis**: Wenn Sie DES oder 3DES verwenden, müssen Sie den Befehl **ssh host-key ip_address** verwenden, um den SSH-Schlüssel vom Gerät zu akzeptieren.
6. Geben Sie die NAT-Adresse des Sensors an.
`sensor(config-net-rou)#`**`nat-address`** *`nat_address`*
Hinweis: Dadurch wird die IP-Adresse in der ersten Zeile der ACL von der Adresse des Sensors in die NAT-Adresse geändert. Die NAT-Adresse ist die Sensoradresse nach NAT, die von einem zwischengeschalteten Gerät zwischen dem Sensor und dem Blockierungsgerät übersetzt wird.
7. Geben Sie an, ob der Router Blockierung, Ratenbegrenzung oder beides durchführt.**Hinweis**: Der Standardwert ist "Blockierung". Sie müssen keine Antwortfunktionen konfigurieren, wenn der Router nur blockiert werden soll.Nur Ratenbegrenzung
`sensor(config-net-rou)#`**`response-capabilities rate-limit`**

   Blockierung und Ratenbegrenzung
`sensor(config-net-rou)#`**`response-capabilities block|rate-limit`**

8. Geben Sie den Namen und die Richtung der Schnittstelle an.
`sensor(config-net-rou)#`**`block-interfaces`** *`interface_name`* **`{in | out}`**

   Hinweis: Der Name der Schnittstelle muss eine Abkürzung sein, die der Router erkennt, wenn er nach dem Befehl **interface** verwendet wird.
9. (Optional) Fügen Sie den Namen vor der ACL hinzu (nur Blockierung).
`sensor(config-net-rou-blo)#`**`pre-acl-name`** *`pre_acl_name`*
10. (Optional) Fügen Sie den Namen nach der ACL hinzu (nur Blockierung).
`sensor(config-net-rou-blo)#`**`post-acl-name`** *`post_acl_name`*
11. Überprüfen Sie die Einstellungen.

```
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. Beenden Sie den Submodus für den Netzwerkzugriff.
```
sensor(config-net-rou)#exit
sensor(config-net)#exit
sensor(config)#exit
Apply Changes:?[yes]:
```
13. Drücken Sie die Eingabetaste, um die Änderungen anzuwenden, oder geben Sie no ein, um sie zu verwerfen.

Konfigurieren des Sensors für die Verwaltung von Cisco Firewalls

Gehen Sie wie folgt vor, um den Sensor für die Verwaltung von Cisco Firewalls zu konfigurieren:

1. Melden Sie sich bei der CLI mit einem Konto mit Administratorrechten an.
2. Wechseln Sie in den Submodus für den Netzwerkzugriff.
```
sensor#configure terminal
sensor(config)#service network-access
sensor(config-net)#
```
3. Geben Sie die IP-Adresse für die von ARC gesteuerte Firewall an.
```
sensor(config-net)#firewall-devices ip_address
```
4. Geben Sie den Benutzerprofilnamen ein, den Sie bei der Konfiguration des Benutzerprofils erstellt haben.
```
sensor(config-net-fir)#profile-name user_profile_name
```
Hinweis: ARC akzeptiert alle von Ihnen eingegebenen Daten. Es wird nicht überprüft, ob das logische Gerät vorhanden ist.
5. Geben Sie die Methode für den Zugriff auf den Sensor an.
```
sensor(config-net-fir)#communication {telnet | ssh-des | ssh-3des}
```

Bei nicht spezifizierter Variante wird SSH 3DES verwendet.Hinweis: Wenn Sie DES oder 3DES verwenden, müssen Sie den Befehl ssh host-key ip_address verwenden, um den Schlüssel zu akzeptieren, oder ARC kann keine Verbindung zum Gerät herstellen.
6. Geben Sie die NAT-Adresse des Sensors an.
```
sensor(config-net-fir)#nat-address nat_address
```
Hinweis: Dadurch wird die IP-Adresse in der ersten Zeile der ACL von der IP-Adresse des Sensors in die NAT-Adresse geändert. Die NAT-Adresse ist die Sensoradresse nach NAT, die von einem zwischengeschalteten Gerät zwischen dem Sensor und dem Blockierungsgerät übersetzt wird.
7. Beenden Sie den Submodus für den Netzwerkzugriff.
```
sensor(config-net-fir)#exit
sensor(config-net)#exit
sensor(config)#exit
Apply Changes:?[yes]:
```
8. Drücken Sie die Eingabetaste, um die Änderungen anzuwenden, oder geben Sie no ein, um sie zu verwerfen.

Blockierung mit SHUN in PIX/ASA

Wenn der Befehl shun ausgegeben wird, werden Verbindungen von einem angreifenden Host blockiert. Pakete, die mit den Werten im Befehl übereinstimmen, werden verworfen und protokolliert, bis die Blockierungsfunktion entfernt wird. Das Shun wird unabhängig davon angewendet, ob eine Verbindung mit der angegebenen Hostadresse aktuell aktiv ist.

Wenn Sie die Zieladresse, Quell- und Zielports und das Protokoll angeben, beschränken Sie das Shun auf Verbindungen, die diesen Parametern entsprechen. Sie können nur einen Befehl **shun** für jede Quell-IP-Adresse haben.

Da der Befehl **shun** verwendet wird, um Angriffe dynamisch zu blockieren, wird er nicht in der Konfiguration der Sicherheitsappliance angezeigt.

Wenn eine Schnittstelle entfernt wird, werden alle Shuns, die an diese Schnittstelle angeschlossen sind, ebenfalls entfernt.

Dieses Beispiel zeigt, dass der beleidigende Host (10.1.1.27) eine Verbindung mit dem Opfer (10.2.2.89) zu TCP herstellt. Die Verbindungstabelle der Security Appliance lautet wie folgt:

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

Um Verbindungen von einem angreifenden Host zu blockieren, verwenden Sie den Befehl **shun** im privilegierten EXEC-Modus. Wenden Sie den Befehl **shun** mit den folgenden Optionen an:

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

Der Befehl löscht die Verbindung aus der Verbindungstabelle der Security Appliance und verhindert außerdem, dass Pakete von 10.1.1.27:555 bis 10.2.2.89:666 (TCP) die Sicherheits-Appliance durchlaufen.

Zugehörige Informationen

- Konfigurieren des Sensors für die Verwaltung von Catalyst Switches der Serie 6500 und Cisco Routern der Serie 7600
- Technischer Support und Dokumentation - Cisco Systems