Konfigurieren der Bedrohungserkennung für Remote Access-VPN auf Secure Firewall ASA

Inhalt

Einleitung

In diesem Dokument wird der Prozess der Konfiguration von Funktionen zur Erkennung von Sicherheitsrisiken für Remote Access VPN auf der Cisco Secure Firewall ASA beschrieben.

Hintergrundinformationen

Funktionen zur Erkennung von Sicherheitsrisiken für Remotezugriff-VPN-Dienste ermöglichen Ihnen den Schutz vor den folgenden Szenarien:

1. Verbindungsversuche zur Ungültigerklärung von Remotezugriff-VPN-Services. Das heißt, es wird versucht, eine Verbindung zu Diensten herzustellen, die nur für den internen Gebrauch bestimmt sind.
2. Client-Initiation-Angriffe, bei denen der Angreifer die Verbindungsversuche mit einem VPN-Headend für den Fernzugriff startet, jedoch nicht abschließt, und zwar wiederholt von einem einzelnen Host aus.
3. Wiederholte fehlgeschlagene Authentifizierungsversuche für Remotezugriff-VPN-Dienste (Brute-Force-Angriffe mit Benutzername/Kennwort).

Diese Angriffe können selbst dann, wenn sie keinen Zugriff erhalten, Rechenressourcen belegen und verhindern, dass gültige Benutzer eine Verbindung zu den Remotezugriffs-VPN-Diensten herstellen.

Wenn Sie diese Dienste aktivieren, führt die sichere Firewall automatisch eine Warnung für den Host (die IP-Adresse) aus, der die konfigurierten Schwellenwerte überschreitet, um weitere

Versuche zu verhindern, bis Sie die Warnung für die IP-Adresse manuell entfernen.

Hinweis: Alle Dienste zur Erkennung von Sicherheitsrisiken für das Remotezugriffs-VPN sind standardmäßig deaktiviert.

Voraussetzungen

Cisco empfiehlt Ihnen, sich mit folgenden Themen vertraut zu machen:

- Cisco Secure Firewall Adaptive Security Appliance (ASA)
- Remote Access VPN (RAVPN) auf ASA

Anforderungen

Diese Funktionen zur Erkennung von Sicherheitsrisiken werden von den nachfolgend aufgeführten Versionen der Cisco Secure Firewall ASA unterstützt:

- Version 9.16 train -> unterstützt in Version 9.16(4)67 und neueren Versionen
- Version 9.20 train -> unterstützt in Version 9.20(3) und neueren Versionen

Verwendete Komponenten

Die in diesem Dokument beschriebenen Informationen basieren auf den folgenden Hardware- und Softwareversionen:

- Cisco Secure Firewall ASA Version 9.20(3)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Melden Sie sich im globalen Konfigurationsmodus bei der Secure Firewall Command Line Interface (CLI) an, und aktivieren Sie einen oder mehrere der verfügbaren Dienste zur Erkennung von Sicherheitsrisiken für das Remotezugriffs-VPN:

Erkennung von Bedrohungen für Verbindungsversuche mit internen (ungültigen) VPN-Services

Führen Sie zum Aktivieren dieses Diensts den Befehl invalid-vpn-access des Diensts zur Erkennung von Sicherheitsrisiken aus.

Erkennung von Sicherheitsrisiken bei Initiierung von Angriffen durch VPN-Clients mit Remote-Zugriff

Um diesen Dienst zu aktivieren, führen Sie den Befehl Threat Detection Service remote-access-client-initiations hold-down <minutes> threshold <count> aus, wobei:

- hold-down <Minuten> definiert den Zeitraum nach dem letzten Initiierungsversuch, in dem aufeinander folgende Verbindungsversuche gezählt werden. Wenn die Anzahl der aufeinander folgenden Verbindungsversuche den konfigurierten Grenzwert innerhalb dieses Zeitraums erreicht, wird die IPv4-Adresse des Angreifers ignoriert. Sie können diesen Zeitraum zwischen 1 und 1440 Minuten einstellen.
- threshold <count> ist die Anzahl der Verbindungsversuche, die innerhalb der Haltezeit erforderlich sind, um einen Shun auszulösen. Sie können einen Schwellenwert zwischen 5 und 100 festlegen.

Beträgt die Haltezeit beispielsweise 10 Minuten und der Grenzwert 20 Minuten, wird die IPv4-Adresse automatisch ignoriert, wenn innerhalb von 10 Minuten 20 aufeinander folgende Verbindungsversuche unternommen werden.

Hinweis: Bei der Festlegung der Hold-Down- und Schwellenwerte ist die NAT-Nutzung zu berücksichtigen. Wenn Sie PAT verwenden, wodurch viele Anfragen von derselben IP-Adresse möglich sind, sollten Sie höhere Werte in Betracht ziehen. Dadurch wird sichergestellt, dass gültigen Benutzern genügend Zeit für eine Verbindung zur Verfügung steht. In einem Hotel können beispielsweise zahlreiche Benutzer in kurzer Zeit versuchen, eine Verbindung herzustellen.

Erkennung von Sicherheitsrisiken bei VPN-Authentifizierungsfehlern für den Remote-Zugriff

Führen Sie zum Aktivieren dieses Dienstes den Befehl Threat Detection Service Remote-Access-Authentication Hold-Down<Minuten> Schwellenwert <count> aus, wobei Folgendes gilt:

- hold-down <Minuten> definiert den Zeitraum nach dem letzten fehlgeschlagenen Versuch, in dem aufeinander folgende Fehler gezählt werden. Wenn die Anzahl der aufeinander folgenden Authentifizierungsfehler den konfigurierten Grenzwert innerhalb dieses Zeitraums erreicht, wird die IPv4-Adresse des Angreifers ignoriert. Sie können diesen Zeitraum zwischen 1 und 1440 Minuten einstellen.
- threshold <count> ist die Anzahl der fehlgeschlagenen Authentifizierungsversuche, die innerhalb der Haltezeit erforderlich sind, um einen Shun auszulösen. Sie können einen Schwellenwert zwischen 1 und 100 festlegen.

Beträgt die Haltezeit beispielsweise 10 Minuten und der Schwellenwert 20, wird die IPv4-Adresse

automatisch ignoriert, wenn innerhalb von 10 Minuten 20 aufeinander folgende Authentifizierungsfehler auftreten.

Hinweis: Bei der Festlegung der Hold-Down- und Schwellenwerte ist die NAT-Nutzung zu berücksichtigen. Wenn Sie PAT verwenden, wodurch viele Anfragen von derselben IP-Adresse möglich sind, sollten Sie höhere Werte in Betracht ziehen. Dadurch wird sichergestellt, dass gültigen Benutzern genügend Zeit für eine Verbindung zur Verfügung steht. In einem Hotel können beispielsweise zahlreiche Benutzer in kurzer Zeit versuchen, eine Verbindung herzustellen.

Hinweis: Authentifizierungsfehler über SAML werden noch nicht unterstützt.

Die nächste Beispielkonfiguration aktiviert die drei verfügbaren Dienste zur Erkennung von Sicherheitsrisiken für das Remotezugriffs-VPN mit einer Haltezeit von 10 Minuten und einem Schwellenwert von 20 für Clientinitiierungsversuche und fehlgeschlagene Authentifizierungsversuche.

```
threat-detection service invalid-vpn-access
threat-detection service remote-access-client-initiations hold-down 10 threshold 20
threat-detection service remote-access-authentication hold-down 10 threshold 20
```

Überprüfung

Um Statistiken für RAVPN-Dienste zur Erkennung von Bedrohungen anzuzeigen, führen Sie den Befehl show threat-detection service [service] [entries|details] aus. Dabei kann es sich um folgenden Dienst handeln: remote-access-authentication, remote-access-client-initiations oder invalid-vpn-access.

Sie können die Ansicht weiter einschränken, indem Sie die folgenden Parameter hinzufügen:

- Einträge - Zeigt nur die Einträge an, die vom Bedrohungserkennungsdienst verfolgt werden. Beispielsweise die IP-Adressen, bei denen die Authentifizierung fehlgeschlagen ist.
- details - Zeigt sowohl Servicedetails als auch Serviceeinträge an.

Führen Sie den Befehl show threat-detection service (Dienst zur Erkennung von Bedrohungen anzeigen) aus, um Statistiken aller aktivierten Dienste zur Erkennung von Bedrohungen anzuzeigen.

```
ciscoasa# show threat-detection service
```

```
Service: invalid-vpn-access
    State     : Enabled
    Hold-down : 1 minutes
    Threshold : 1
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
    Total entries: 2
Name: remote-access-client-initiations
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
```

Um weitere Details zu potenziellen Angreifern anzuzeigen, die für den Remote-Authentifizierungsdienst verfolgt werden, führen Sie den Befehl show threat-detection service <service> entries aus.

```
ciscoasa# show threat-detection service remote-access-authentication entries
Service: remote-access-authentication
    Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1        721         0
  2 192.168.100.102/ 32              outside              2        486       114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

Führen Sie den Befehl show threat-detection service <service> details aus, um die allgemeinen Statistiken und Details zu einem bestimmten Remotezugriffs-VPN-Dienst für die Erkennung von Bedrohungen anzuzeigen.

```
ciscoasa# show threat-detection service remote-access-authentication details
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
     Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1         721           0
  2 192.168.100.102/ 32              outside              2         486         114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

Hinweis: In den Einträgen werden nur die IP-Adressen angezeigt, die vom Dienst zur Erkennung von Sicherheitsrisiken verfolgt werden. Wenn eine IP-Adresse die Bedingungen erfüllt, die vermieden werden sollen, erhöht sich die Blockierungsanzahl, und die IP-Adresse wird nicht mehr als Eintrag angezeigt.

Darüber hinaus können Sie Shuns überwachen, die von den VPN-Diensten angewendet werden, und Shuns für eine einzelne IP-Adresse oder alle IP-Adressen entfernen, indem Sie die folgenden Befehle ausführen:

- show shun [ip_address]

Zeigt nicht autorisierte Hosts an, einschließlich Hosts, die automatisch durch die Erkennung von Sicherheitsrisiken für VPN-Services oder manuell mithilfe des Befehls "shun" ausgeschlossen werden. Optional können Sie die Ansicht auf eine bestimmte IP-Adresse beschränken.

- no shun ip_address [interface if_name]

Entfernt den Shun nur von der angegebenen IP-Adresse. Sie können optional den Schnittstellennamen für die Weiterleitung angeben, wenn die Adresse auf mehr als einer Schnittstelle weitergeleitet wird und Sie die Weiterleitung auf einigen Schnittstellen beibehalten möchten.

- Klarsichtzeichen

Entfernt die Verknüpfung von allen IP-Adressen und Schnittstellen.

Hinweis: IP-Adressen, die von der Erkennung von Sicherheitsrisiken für VPN-Services ausgeschlossen werden, werden nicht im Befehl show threat-detection shun angezeigt, der nur für die Suche nach Sicherheitsrisiken gilt.

Weitere Informationen zu den einzelnen Befehlen und verfügbaren Syslog-Meldungen zu den Erkennungsdiensten für Remote-Access-VPNs finden Sie im Cisco Secure Firewall ASA Firewall CLI Configuration Guide, 9.20. Kapitel: Dokument zur Erkennung von Bedrohungen.

Zugehörige Informationen

- Wenden Sie sich für zusätzliche Unterstützung an das Technical Assistance Center (TAC). Ein gültiger Support-Vertrag ist erforderlich: Weltweiter Kontakt für den Cisco Support.
- Sie können auch die Cisco VPN-Community hier besuchen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.