Fehler beim Abbruch des NGFW-Servicemodule für TLS aufgrund eines Handshake-Fehlers oder eines Zertifikatsvalidierungsfehlers

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Problem Lösung Problem Lösung Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie Sie ein bestimmtes Problem beim Zugriff auf HTTPSbasierte Websites mithilfe des Cisco NGFW-Dienstmoduls (Next-Generation Firewall) mit aktivierter Entschlüsselung beheben können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Secure Sockets Layer (SSL)-Handshake-Verfahren
- SSL-Zertifikate

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco NGFW-Dienstmodul mit Cisco Prime Security Manager (PRSM) Version 9.2.1.2(52).

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.

Hintergrundinformationen

Die Entschlüsselung ist eine Funktion, mit der das NGFW-Dienstmodul SSL-verschlüsselte Datenflüsse entschlüsseln (und die ansonsten verschlüsselte Konversation prüfen) und Richtlinien für den Datenverkehr durchsetzen kann. Um diese Funktion zu konfigurieren, müssen Administratoren ein Entschlüsselungszertifikat auf dem NGFW-Modul konfigurieren, das den HTTPS-basierten Websites für den Client-Zugriff anstelle des ursprünglichen Serverzertifikats angezeigt wird.

Damit die Entschlüsselung funktioniert, muss das NGFW-Modul dem vom Server präsentierten Zertifikat vertrauen. In diesem Dokument werden die Szenarien erläutert, in denen das SSL-Handshake zwischen dem NGFW-Dienstmodul und dem Server ausfällt, wodurch bestimmte HTTPS-basierte Websites fehlschlagen, wenn Sie versuchen, diese zu erreichen.

Für die Zwecke dieses Dokuments werden diese Richtlinien auf dem NGFW-Dienstmodul mit PRSM definiert:

- Identitätsrichtlinien: Es gibt keine definierten Identitätsrichtlinien.
- Entschlüsselungsrichtlinien: Die Entschlüsselungsrichtlinie verwendet folgende Konfiguration:

alta cisc	o Secu	Prime rity Manag	er					Quick	start Help admin Logout
De	hiboard	Events	Configurations	Componenta	Administration				NO PENDING CHANGES
Polio	ies/Settings	Cortific	otos Updatos	Monitor-only mode					
0.00	1		Entr	r fiter oriteria	Annual and data		× • Fiber		
United and	iym	1 4001	earts x	neoxinos neorida i x	Access borces		Decryption policies 12 Control		
1	=	A+ Name		Source	Des	tination	Service	Action	Interface roles
C* .	1	▼ Decrypt	lon_ASA_ASA_ASA (1)				Default D	ecryption Policy Set
1		1 Decrypt-/	đ	Acq	Aty		Ary	Averys decrypt for inspection	Any to Any
ų,									
x									

- Zugriffsrichtlinien: Es gibt keine definierten Zugriffsrichtlinien.
- Entschlüsselungseinstellungen: In diesem Dokument wird davon ausgegangen, dass ein Entschlüsselungszertifikat auf dem NGFW-Dienstmodul konfiguriert ist und dass die Clients ihm vertrauen.

Wenn eine Entschlüsselungsrichtlinie auf dem NGFW-Dienstmodul definiert und wie zuvor beschrieben konfiguriert wurde, versucht das NGFW-Dienstmodul, den gesamten SSL-verschlüsselten Datenverkehr über das Modul abzufangen und zu entschlüsseln.

Hinweis: Eine schrittweise Erläuterung dieses Prozesses finden Sie im Abschnitt <u>Entschlüsselter Datenverkehrsfluss</u> im <u>Benutzerhandbuch für ASA CX und Cisco Prime</u> <u>Security Manager 9.2</u>.

Dieses Bild zeigt die Abfolge der Ereignisse:



In diesem Image **ist A** der Client, **B** das NGFW-Dienstmodul und **C** der HTTPS-Server. Für die in diesem Dokument gezeigten Beispiele ist der HTTPS-basierte Server ein Cisco Adaptive Security Device Manager (ASDM) auf einer Cisco Adaptive Security Appliance (ASA).

Bei diesem Prozess sollten Sie zwei wichtige Faktoren berücksichtigen:

- Im zweiten Schritt des Prozesses muss der Server eine der SSL-Verschlüsselungssuiten akzeptieren, die vom NGFW-Dienstmodul bereitgestellt werden.
- Im vierten Schritt des Prozesses muss das NGFW-Servicemodul dem vom Server bereitgestellten Zertifikat vertrauen.

Problem

Wenn der Server keine der SSL-Chiffren akzeptieren kann, die vom NFGW-Dienstmodul bereitgestellt werden, erhalten Sie eine Fehlermeldung, die der folgenden ähnelt:

TLS Abort	Event	D
-----------	-------	---

A TLS or SSL flow was aborted due to a handshake failure or certificate validation error.

		Destination		Transaction	
User		IP address	172.16.1.1	Connection ID	390891
Realm		Port	443	Transaction ID	
P address	10.1.1.10	Interface	Idap	Component name	TLS Proxy
Port	64193	Service	tcp/443	Bytes sent	179
Interface inside		Host		Bytes received	7
Identity		URL:		Total bytes	186
Remote device No		URL category		Request content type	
Client OS name		Web reputation		Response content	
Context name		Threat type		type:	
				HTTP response status	
LS		Application		HTTP app detected	
Encrypted flow:	Yes	Name	Transport Layer Security	Configuration version	89
Decrypted flow	No		Protocol	Error details	00
Requested domain		Type	IP Protocol		
Ambiguous destination		Benavior			
Server certificate name		Device			
		Name	ASA – CX		
Server certificate issuer		Туре	ASA-CX		
TLS version					
Server cipher suite					
Error Details	error:14077410:SSL routines:SSL23_GET_SERVER_ HELLO:sslv3 alert handshake failure				

Beachten Sie unbedingt die Informationen zu Fehlerdetails (hervorgehoben), die Folgendes zeigen:

error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:**sslv3 alert handshake failure** Wenn Sie die Datei **/var/log/cisco/tls_proxy.log** im Moduldiagnosearchiv anzeigen, werden folgende Fehlermeldungen angezeigt:

2014-02-05 05:21:42,189 INFO TLS_Proxy - SSL alert message received from server (0x228 = "fatal : handshake failure") in Session: x2fd1f6 2014-02-05 05:21:42,189 ERROR TLS_Proxy - TLS problem (error:14077410: SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure) while connecting to server for Session: x2fd1f6

Lösung

Eine mögliche Ursache für dieses Problem ist, dass eine Triple Data Encryption Standard/Advanced Encryption Standard (3DES/AES)-Lizenz (häufig auch als K9 bezeichnet) nicht auf dem Modul installiert ist. Sie können <u>die K9-Lizenz</u> für das Modul kostenlos <u>herunterladen</u> und über PRSM hochladen.

Wenn das Problem weiterhin besteht, nachdem Sie die 3DES/AES-Lizenz installiert haben, rufen Sie die Paketerfassung für den SSL-Handshake zwischen dem NGFW-Dienstmodul und dem Server ab, und wenden Sie sich an den Serveradministrator, um die entsprechende(n) SSL-Chiffre(n) auf dem Server zu aktivieren.

Close

Problem

Wenn das NGFW-Dienstmodul dem vom Server bereitgestellten Zertifikat nicht traut, erhalten Sie eine Fehlermeldung ähnlich der folgenden:

Event details						
Source		Destination		Transaction		
User		IP address	172.16.1.1	Connection ID	390874	
Realm		Port	443	Transaction ID		
IP address	10.1.1.10	Interface	Idap	Component name	TLS Proxy	
Port	64186	Service	tcp/443	Bytes sent	186	
Interface	inside	Host		Bytes received	523	
Identity		URL:		Total bytes	709	
Remote device	No	URL category		Request content type		
Client OS name		Web reputation		Response content		
Context name		Threat type		type:		
ILS		Application		HTTP response status HTTP app detected		
Encrypted flow:	Yes	Name	Transport Layer Security	phase Crafterenting services	60	
Decrypted flow	No		Protocol	Computation Version	09	
Requested domain		Туре	IP Protocol	Error cetaits		
Ambiguous destination		Behavior				
Server certificate		Device				
name		Name	ASA – CX			
Server certificate issuer	/unstructuredName=ciscoasa	Туре	ASA-CX			
TLS version	TLSv1					
Server cipher suite						
Error Details	error:14090066:SSL routines:SSL3_GET_SERVER_C ERTIFICATE:certificate verify failed					

Beachten Sie unbedingt die Informationen zu Fehlerdetails (hervorgehoben), die Folgendes zeigen:

error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed Wenn Sie die Datei /var/log/cisco/tls_proxy.log im Moduldiagnosearchiv anzeigen, werden folgende Fehlermeldungen angezeigt:

2014-02-05 05:22:11,505 INFO TLS_Proxy - Certificate verification failure: self signed certificate (code 18, depth 0) 2014-02-05 05:22:11,505 INFO TLS_Proxy - Subject: /unstructuredName=ciscoasa 2014-02-05 05:22:11,505 INFO TLS_Proxy - Issuer: /unstructuredName=ciscoasa 2014-02-05 05:22:11,505 INFO TLS_Proxy - SSL alert message received from server (0x230 = "fatal : unknown CA") in Session: x148a696e 2014-02-05 05:22:11,505 ERROR TLS_Proxy - TLS problem (error:14090086: SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed) while

connecting to server for Session: x148a696e

Lösung

Wenn das Modul dem SSL-Serverzertifikat nicht vertrauen kann, müssen Sie das Serverzertifikat mit PRSM in das Modul importieren, um sicherzustellen, dass der SSL-Handshake-Prozess erfolgreich ist.

Gehen Sie wie folgt vor, um das Serverzertifikat zu importieren:

 Umgehen Sie das NGFW-Dienstmodul, wenn Sie auf den Server zugreifen, um das Zertifikat über einen Browser herunterzuladen. Eine Möglichkeit, das Modul zu umgehen, besteht darin, eine Entschlüsselungsrichtlinie zu erstellen, die den Datenverkehr zu diesem bestimmten Server nicht entschlüsselt. In diesem Video erfahren Sie, wie Sie die Richtlinie erstellen:

Dies sind die Schritte, die im Video gezeigt werden:

Um auf das PRSM in der CX zuzugreifen, navigieren Sie zu https://<IP_ADDRESS_OF_PRSM>. In diesem Beispiel wird https://10.106.44.101 verwendet.

Navigieren Sie zu Konfigurationen > Richtlinien/Einstellungen > Entschlüsselungsrichtlinien im PRSM.

Klicken Sie auf das Symbol in der linken oberen Ecke des Bildschirms, und wählen Sie die Option **Oben** hinzugefügte **Richtlinie** aus, um eine Richtlinie zum Anfang der Liste hinzuzufügen.

Benennen Sie die Richtlinie, belassen Sie die Quelle als Any, und erstellen Sie ein CX-Netzwerkgruppenobjekt.

Hinweis: Denken Sie daran, die IP-Adresse des HTTPS-basierten Servers einzuschließen. In diesem Beispiel wird die IP-Adresse **172.16.1.1** verwendet.Wählen Sie **Entschlüsseln Sie** nicht für die Aktion.

Speichern Sie die Richtlinie, und bestätigen Sie die Änderungen.

2. Laden Sie das Serverzertifikat über einen Browser herunter und laden Sie es über PRSM auf das NGFW-Dienstmodul hoch, wie in diesem Video gezeigt:

Dies sind die Schritte, die im Video gezeigt werden:

Nachdem die zuvor genannte Richtlinie definiert wurde, navigieren Sie mithilfe eines Browsers zum HTTPS-basierten Server, der über das NGFW-Dienstmodul geöffnet wird. **Hinweis**: In diesem Beispiel wird Mozilla Firefox Version 26.0 verwendet, um zum Server (einem ASDM auf einer ASA) mit der URL **https://172.16.1.1** zu navigieren.Nehmen Sie die Sicherheitswarnung an, wenn ein Fenster geöffnet wird, und fügen Sie eine Sicherheitsausnahme hinzu.

Klicken Sie links neben der Adressleiste auf das kleine blockförmige Symbol. Die Position dieses Symbols hängt vom verwendeten Browser und der Version ab.

Klicken Sie auf die Schaltfläche **Zertifikat anzeigen** und anschließend auf der Registerkarte Details auf die Schaltfläche **Exportieren**, nachdem Sie das Serverzertifikat ausgewählt haben.

Speichern Sie das Zertifikat an einem beliebigen Ort auf Ihrem PC.

Melden Sie sich beim PRSM an, und wählen Sie Konfigurationen > Zertifikate aus.

Klicken Sie auf **Ich möchte ... > Zertifikat importieren** und zuvor heruntergeladenes Serverzertifikat (aus Schritt 4) auswählen.

Speichern und bestätigen Sie die Änderungen. Nach Abschluss dieses Vorgangs sollte das NGFW-Servicemodul dem vom Server vorgelegten Zertifikat vertrauen.

3. Entfernen Sie die Richtlinie, die in Schritt 1 hinzugefügt wurde. Das NGFW-Servicemodul kann nun den Handshake mit dem Server erfolgreich abschließen.

Zugehörige Informationen

- Benutzerhandbuch für ASA CX und Cisco Prime Security Manager 9.2
- <u>Technischer Support und Dokumentation Cisco Systems</u>