Konfigurieren der SSL-Entschlüsselung auf dem FirePOWER-Modul mithilfe von ASDM (integriertes Management)

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Ausgehende SSL-Entschlüsselung Eingehende SSL-Entschlüsselung Konfiguration für SSL-Entschlüsselung Entschlüsselung ausgehender SSL-Verbindungen (Entschlüsseln - Zurücksetzen) Schritt 1: Konfigurieren Sie das CA-Zertifikat. Schritt 2: Konfigurieren Sie die SSL-Richtlinie. Schritt 3: Konfigurieren der Zugriffskontrollrichtlinie Eingehende SSL-Entschlüsselung (Entschlüsseln - bekannt) Schritt 1: Importieren Sie das Serverzertifikat und den Serverschlüssel. Schritt 2: Importieren Sie das Zertifizierungsstellenzertifikat (optional). Schritt 3: Konfigurieren Sie die SSL-Richtlinie. Schritt 4: Konfigurieren Sie die Zugriffskontrollrichtlinie. Überprüfen Fehlerbehebung Zugehörige Informationen

Einführung

Dieses Dokument beschreibt die Konfiguration der SSL-Entschlüsselung (Secure Sockets Layer) auf dem FirePOWER-Modul mithilfe von ASDM (On-Box Management).

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnis der ASA-Firewall (Adaptive Security Appliance), ASDM (Adaptive Security Device Manager)
- Kenntnis der FirePOWER-Appliance
- Kenntnis des HTTPS/SSL-Protokolls

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASA FirePOWER-Module (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) mit Softwareversion 6.0.0 und höher
- ASA FirePOWER-Modul (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X) mit Softwareversion 6.0.0 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: Stellen Sie sicher, dass das FirePOWER-Modul über eine **Protect**-Lizenz verfügt, um diese Funktion zu konfigurieren. Um die Lizenz zu überprüfen, wählen Sie **Configuration > ASA FirePOWER Configuration > License aus**.

Hintergrundinformationen

Das FirePOWER-Modul entschlüsselt und prüft ein- und ausgehende SSL-Verbindungen, die an das Modul umgeleitet werden. Sobald der Datenverkehr entschlüsselt ist, werden getunnelte Anwendungen wie Facebook-Chat usw. erkannt und kontrolliert. Die entschlüsselten Daten werden auf Bedrohungen, URL-Filterung, Dateiblockierung oder schädliche Daten geprüft.

Ausgehende SSL-Entschlüsselung

Das Firepower-Modul fungiert als Forward-Proxy für ausgehende SSL-Verbindungen, indem es ausgehende SSL-Anfragen abfängt und ein Zertifikat für die Site wiederherstellt, die der Benutzer besuchen möchte. Die ausstellende Behörde (CA) ist das selbstsignierte FirePOWER-Zertifikat. Wenn das Zertifikat der Firewall nicht Teil einer bestehenden Hierarchie ist oder nicht zum Browser-Cache eines Clients hinzugefügt wird, erhält der Client beim Navigieren zu einer sicheren Website eine Warnung. Die Entschlüsselungsmethode wird zum Durchführen der SSL-Entschlüsselung für ausgehenden Datenverkehr verwendet.

Eingehende SSL-Entschlüsselung

Bei eingehenden Datenverkehr zu einem internen Webserver oder Gerät importiert der Administrator eine Kopie des Zertifikats und des Schlüssels des geschützten Servers. Wenn das SSL-Serverzertifikat auf das Firepower-Modul geladen wird und die SSL-Verschlüsselungsrichtlinie für den eingehenden Datenverkehr konfiguriert wird, entschlüsselt und prüft das Gerät den Datenverkehr beim Weiterleiten. Das Modul erkennt dann schädliche Inhalte, Bedrohungen und Malware, die über diesen sicheren Kanal übertragen werden. Darüber hinaus wird die Entschlüsselungsmethode verwendet, um eine eingehende SSL-Entschlüsselung durchzuführen.

Konfiguration für SSL-Entschlüsselung

Es gibt zwei Methoden zur Entschlüsselung des SSL-Datenverkehrs.

- Entschlüsseln Für ausgehenden SSL-Datenverkehr kündigen
- Entschlüsseln Bekannt für eingehenden SSL-Datenverkehr

Entschlüsselung ausgehender SSL-Verbindungen (Entschlüsseln - Zurücksetzen)

Das FirePOWER-Modul fungiert als MITM (Man-in-the-Middle) für alle SSL-Verhandlungen für öffentliche SSL-Server. Das Zertifikat des öffentlichen Servers wird mit einem Zwischenzertifikat der Zertifizierungsstelle zurückgesendet, das auf dem Firepower-Modul konfiguriert ist.

Dies sind die drei Schritte zum Konfigurieren der ausgehenden SSL-Entschlüsselung.

Schritt 1: Konfigurieren Sie das CA-Zertifikat.

Konfigurieren Sie entweder ein selbstsigniertes Zertifikat oder ein zwischengeschaltetes vertrauenswürdiges Zertifizierungsstellen-Zertifikat für den Zertifikatsrücktritt.

Konfigurieren des selbstsignierten Zertifizierungsstellenzertifikats

Um das selbst signierte CA-Zertifikat zu konfigurieren, navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Object Management > PKI > Internal CAs** und klicken Sie auf **Generate CA (CA generieren)**. Das System fordert Sie zur Eingabe der Details des Zertifizierungsstellenzertifikats auf. Wie im Bild gezeigt, füllen Sie die Details entsprechend Ihrer Anforderungen aus.

ASA FirePOWER Configur 🗗 👎	Configuration > ASA FirePOWER Configuration > Object Management > PKI > Internal CAs
	Name Generate Internal Certificate Authority ? × Name: ServerCA Country Name (two-letter code): IN State or Province: KA Locality or City: Bangalore Organizational Unit (Department): TAC Common Name: serverCA.example.com
Firewall	Generate CSR Generate self-signed CA Cancel No data to display < < Pa
Site-to-Site VPN	

Klicken Sie auf **Eigensignierte CA erstellen**, um das interne Zertifizierungsstellenzertifikat zu generieren. Klicken Sie anschließend auf **CSR erstellen**, um die Zertifikatssignierungsanfrage zu generieren, die dann zur Signierung an den CA-Server weitergegeben wird.

Konfigurieren des Zertifikats der vermittelten Zertifizierungsstelle

Um das von einer anderen CA signierte Zertifikat der Zwischen-Zertifizierungsstelle zu konfigurieren, navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Object Management > PKI > Internal CAs** und klicken Sie auf **Import CA**.

Geben Sie den Namen des Zertifikats an. Wählen Sie **Durchsuchen** und Hochladen des Zertifikats vom lokalen Computer aus, oder fügen Sie den Inhalt des Zertifikats in die Option **Zertifikatsdaten** ein. Um den privaten Schlüssel des Zertifikats anzugeben, durchsuchen Sie entweder die Schlüsseldatei, oder fügen Sie den Schlüssel in die **Key-**Option ein.

Wenn der Schlüssel verschlüsselt ist, aktivieren Sie das Kontrollkästchen Verschlüsselt, und geben Sie das Kennwort an. Klicken Sie auf OK, um den Zertifikatsinhalt zu speichern, wie im Bild gezeigt:



Schritt 2: Konfigurieren Sie die SSL-Richtlinie.

Die SSL-Richtlinie definiert die Entschlüsselungsaktion und identifiziert den Datenverkehr, auf den die Entschlüsselungsmethode angewendet wird. Konfigurieren Sie die verschiedenen SSL-Regeln auf Basis Ihrer geschäftlichen Anforderungen und Sicherheitsrichtlinien.

Um die SSL-Richtlinie zu konfigurieren, wählen Sie **Configure > ASA FirePOWER Configuration > Policies > SSL aus,** und klicken Sie auf **Add Rule (Regel hinzufügen)**.

Name: Geben Sie den Namen der Regel an.

Aktion: Geben Sie die Aktion als **Entschlüsseln - Zurückweisen an,** und wählen Sie das Zertifizierungsstellenzertifikat aus der Dropdown-Liste aus, die im vorherigen Schritt konfiguriert wurde.

Definieren Sie in der Regel Bedingungen, um den Datenverkehr abzugleichen, da es mehrere Optionen gibt (Zone, Netzwerk, Benutzer usw.), die zum Definieren des Datenverkehrs, der entschlüsselt werden muss, angegeben werden.

Aktivieren Sie zum Generieren der SSL-Entschlüsselungsereignisse die **Protokollierungsoption**, wie im Bild gezeigt:

O O ASA FirePOWER Configurat	○ ○ ○ Configuration > ASA FirePOWER Configuration > Policies > SSL	
▼ 🗐 Policies		
🚦 Access Control Policy	Default SSL Policy	
Intrusion Policy	SSI Palicy	
Files	out runey	
SSL		26.47
X Actions Alerts		N 12
Lentity Policy	Rules Trusted CA Certificates Undecryptable Actions	
DNS Policy	Add Category Add Category Add Category Add Category	X
Device Management		
Object Management	Add Rule	? ×
Sustam Information		
Indates	Name Outboound_SSL_Decrypt I Enabled Insert into Category Standard Rules	~
Tools	Action Decrypt * Resign • • • • • • Serverce • • • • • • • • • • • • • • • • • • •	
🕨 🍡 Integration	Zones Networks Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version	paging
	Available Networks (* O Source Networks (1) Destination Networks (0)	
	Search by name or value	
	Networks Geolocation	
	Private Networks	
	Add to	
	Source	
	Add to	
	Destination	
A Davice Setup		
Device setup	Enter an 1º address Add Enter an 1º address	Add
Firewall	Add	ancel
Remote Access VPN		
Site-to-Site VPN		2.21.0
ASA FirePOWER Configur	No data to display K K Page 1 of 1	110

Klicken Sie auf Hinzufügen, um die SSL-Regel hinzuzufügen.

Klicken Sie auf **Store ASA FirePOWER Changes**, um die Konfiguration der SSL-Richtlinie zu speichern.

Schritt 3: Konfigurieren der Zugriffskontrollrichtlinie

Wenn Sie die SSL-Richtlinie mit entsprechenden Regeln konfigurieren, müssen Sie die SSL-Richtlinie in der Zugriffskontrolle angeben, um die Änderungen zu implementieren.

Um die Zugriffskontrollrichtlinie zu konfigurieren, navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Policies > Access Control.**

Klicken Sie entweder auf **Keine** der **SSL-Richtlinie** oder navigieren Sie zu **Erweitert > SSL Policy Setting.** Geben Sie die SSL-Richtlinie aus der Dropdown-Liste ein, und klicken Sie auf OK, um sie zu speichern, wie im Bild gezeigt:

O O ASA FirePOWER Configurat	O O O Configuration > ASA FirePOWER Configuration > Policies > Access	<u>Control I</u>
▼		
Access Control Policy	ASA ASA FirePOWER	
Intrusion Policy		
💾 Files	Default Allow All Traffic	
🔒 SSL	Enter a description	
🔯 Actions Alerts		
Lentity Policy		
DNS Policy		
Device Management		
Object Management		
► 🙆 Local	Identity Policy: None SSL Policy: None	
System Information	Rules Security Intelligence HTTP Responses Advanced	
		-
 A Tools 	General Settings	Ø
Integration	Maximum URL characters to store in connection events	1024
	Allow an Interactive Block to hypacs blocking for (coconds)	600
	Allow an interactive block to bypass blocking for (seconds)	000
	Retry U SSL Policy to use for inspecting encrypted ? ×	Yes
	Inspect connections	Yes
	Identit Default SSL Policy	Ø
	Identit Revert to Defaults OK Cancel	None
	SSL Policy Settings	Ø
	SSL Policy to use for inspecting encrypted connections	None

Klicken **ASA FirePOWER-Änderungen speichern** um die Konfiguration der SSL-Richtlinie zu speichern.

Sie müssen die Zugriffskontrollrichtlinie auf dem Sensor bereitstellen. Bevor Sie die Richtlinie anwenden, gibt es Hinweise darauf, dass die Zugriffskontrollrichtlinie auf dem Modul veraltet ist. Um die Änderungen am Sensor bereitzustellen, klicken Sie auf Deploy und wählen Sie die Option Deploy FirePOWER Changes (FirePOWER-Änderungen bereitstellen). Überprüfen Sie die vorgenommenen Änderungen, und klicken Sie auf Bereitstellen.

Hinweis: Wenn Sie in Version 5.4.x die Zugriffsrichtlinie auf den Sensor anwenden möchten, klicken Sie auf **ASA FirePOWER-Änderungen anwenden**.

Hinweis: Navigieren Sie zu **Monitoring > ASA FirePOWER Monitoring > Task Status.** Anschließend beantragen Sie Konfigurationsänderungen, um sicherzustellen, dass die Aufgabe abgeschlossen ist.

Eingehende SSL-Entschlüsselung (Entschlüsseln - bekannt)

Die Methode der eingehenden SSL-Entschlüsselung (Entschlüsselung - bekannt) wird verwendet, um den eingehenden SSL-Datenverkehr zu entschlüsseln, für den Sie ein Serverzertifikat und einen privaten Schlüssel konfiguriert haben. Sie müssen das Serverzertifikat und den privaten Schlüssel in das FirePOWER-Modul importieren. Wenn SSL-Datenverkehr auf das FirePOWER-Modul trifft, entschlüsselt er den Datenverkehr und führt die Überprüfung des entschlüsselten Datenverkehrs durch. Nach der Überprüfung verschlüsselt das FirePOWER-Modul den Datenverkehr neu und sendet ihn an den Server.

Dies sind die vier Schritte zum Konfigurieren der ausgehenden SSL-Entschlüsselung:

Schritt 1: Importieren Sie das Serverzertifikat und den Serverschlüssel.

Um das Serverzertifikat und den Serverschlüssel zu importieren, navigieren Sie zu **Configuration >** ASA FirePOWER Configuration > Object Management > PKI > Internal Certs und klicken Sie auf Add Internal Cert.

Geben Sie, wie im Bild gezeigt, den Namen des Zertifikats an. Wählen Sie entweder **Durchsuchen**, um das Zertifikat vom lokalen Computer auszuwählen, oder fügen Sie den Inhalt des Zertifikats in die **Zertifikatsdaten ein**. Um den privaten Schlüssel des Zertifikats anzugeben, durchsuchen Sie entweder die Schlüsseldatei, oder fügen Sie den Schlüssel in die Option **Schlüssel** ein.

Wenn der Schlüssel verschlüsselt ist, aktivieren Sie das Kontrollkästchen Verschlüsselt, und geben Sie das Kennwort an, wie im Bild gezeigt:

O O ASA FirePOWER Configurat	ent > <u>PKI</u> > <u>Interna</u>	l Certs
Application Filters		
▶ www URL	Add Internal Cert	Eil
GeoLocation	Add Internal Cert	
Na Add Known Internal Certificate		? X
SecurityIntelligence		
Sinkhole Name: web.servertest.com		
📝 FileList		
Certificate Data or, choose a file: Browse		
Istinguished Name nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA0ucjKK9ofSyrAbYkSKC/nvy2g7Mj		
V Q PKI RHbV0UEK+2a5u5fDvZIRURHHBEbFp+SV0E7ak7PljdXd/sB4nhvvfPe4FN65IurN		
Internal CAs Internal CAs High Strain Str		
Trusted CAs Lrcyns+lrbHTJhge0Z2HC/XJmYwyJXhBuEqvU9qx+GhQ99jNCOlo0iPIGF1naqBt		
External Certs		
Internal Certs		
👶 Internal CA Groups		
👫 Trusted CA Groups		
A Internal Cert Group:		
A External Cert Group		
► Local MILCXAIBAAKBGQUSSSYMOrZh9LKSBUKIOL+P/LaDSyMedtXkQQr/Zfm/l8O9knFk EccERsWn5JXOTtoTs+WN1d3+wHieG+9897gU3rki6s2aPNiLBTLiOLv5LM6v/1iE		
System Information OmjP/YjZ29Hi5nU8D0BCpe/J4IIv84JCYVA6s/r6puT4U8ct/3AXEGCGkQIDAQAB		
Updates AoGBAJ+XOAu5cCAIhP6ujZZHzbjJEnNmQvGz2uiVh3HlsfY6SWxR87ic8zRROZBq aNNIWC4zm0R022Cuu2X/zHi46Z7hEar00EaR0482BHu47UEWaga2aaa3allbda10		
Licenses +nzEJwx4LamXR8N88YbkvC3n4iVY5z90fsvCdJ2UoAGBXN4BAkEA+nkDe1UalxOz		
▼ 💼 Tools Pgmzad68lngk4/7Wbg8ibZz0Mv2PSvO7pNbhRfpy/dtgGLJvIGJIr/+0iL2SrPFv		
Image: Starting of Control Starting Startin		
Encrypted, and the password is:		
Device Setup	R Changes Cance	<u> </u>

Klicken Sie auf Store ASA FirePOWER Changes, um den Zertifikatsinhalt zu speichern.

Schritt 2: Importieren Sie das Zertifizierungsstellenzertifikat (optional).

Für ein Serverzertifikat, das vom internen Zwischenzertifikat oder dem Stammzertifikat der Zertifizierungsstelle signiert wird, müssen Sie die interne Kette von Zertifizierungsstellenzertifikaten in das Firepower-Modul importieren. Nach dem Import kann das Firewall-Modul das Serverzertifikat validieren.

Um das CA-Zertifikat zu importieren, navigieren Sie zu **Configuration > ASA Firepower Configuration > Object Management > Trusted CAs** und klicken Sie auf **Add Trusted CA (Vertrauenswürdige CA hinzufügen)**, um das CA-Zertifikat hinzuzufügen.

Schritt 3: Konfigurieren Sie die SSL-Richtlinie.

Die SSL-Richtlinie definiert die Aktion und die Serverdetails, für die Sie die Entschlüsselungsmethode zum Entschlüsseln des eingehenden Datenverkehrs konfigurieren möchten. Wenn Sie über mehrere interne Server verfügen, konfigurieren Sie mehrere SSL-Regeln, die auf unterschiedlichen Servern und dem von ihnen verarbeiteten Datenverkehr basieren.

Um die SSL-Richtlinie zu konfigurieren, wählen Sie **Configure > ASA FirePOWER Configuration > Policies > SSL aus,** und klicken Sie auf **Add Rule (Regel hinzufügen)**.

Name: Geben Sie den Namen der Regel an.

Aktion: Geben Sie die Aktion als **Entschlüsseln - bekannt an** und wählen Sie das Zertifizierungsstellenzertifikat aus der Dropdown-Liste aus, die im vorherigen Schritt konfiguriert wurde.

Definieren Sie die Bedingung, um diese Regeln zu erfüllen, da mehrere Optionen (Netzwerk, Anwendung, Ports usw.) angegeben sind, um den interessanten Datenverkehr des Servers zu definieren, für den Sie die SSL-Entschlüsselung aktivieren möchten. Geben Sie die interne CA auf der Registerkarte **Ausgewählte vertrauenswürdige CAs im Zertifikat für vertrauenswürdige CA an**.

Um die SSL-Entschlüsselungsereignisse zu generieren, aktivieren Sie die Option Loggingat logging.

○ ○ ○ ASA FirePOWER Configurat ○ ○ ○ Configuration > ASA FirePOWER	Configuration > Policies	> SSL			
V D Policies					
SACCESS CONTROL POLICY Default SSL Policy					
▼					
Intrusion Policy					
😼 Rule Editor					3.6 (
Files					
SSL Rules Trusted CA Certificates Undec	yptable Actions				
Actions Alerts					
Add Rule					? X
		Cashlad	• · · · · · · · ·		
Object Management		Enabled	Insert below rule	▶ 1	
Action 🔒 Decrypt - Known Key 💙	web.servertest.com	E	Edit		
▶ Port					
Security Zones Zones Networks Users Applic	ations Ports Category	Certificate DN Cert St	tatus Cipher Suite V	ersion	Logging
Application Filters Available Networks	0	Source Networks (0)		Destination Networks (1)	
URL Search by name or value		any		2 192.168.10.5/32	1
GeoLocation					
Variable Set	lon				
SecurityIntelligence Private Networks					
Sinkhole	Add to Source				
Giphar Suite List					
Distinguished Name	Destination				
V Q PKI					
Internal CAs					
🖶 Trusted CAs					
😑 External Certs					
		Enter an IP address	Add	Enter an IP address	Add
A Device Setup				Add	Cancel

Klicken Sie auf Hinzufügen, um die SSL-Regel hinzuzufügen.

Klicken Sie dann auf "Store ASA FirePOWER Changes", um die Konfiguration der SSL-Richtlinie zu speichern.

Schritt 4: Konfigurieren Sie die Zugriffskontrollrichtlinie.

Wenn Sie die SSL-Richtlinie mit entsprechenden Regeln konfigurieren, müssen Sie die SSL-Richtlinie in der Zugriffskontrolle angeben, um die Änderungen zu implementieren.

Um die Zugriffskontrollrichtlinie zu konfigurieren, navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Policies > Access Control.**

Klicken Sie entweder auf die Option Keine neben SSL Policy (SSL-Richtlinie), oder navigieren Sie zu Advanced > SSL Policy Setting (Erweitert > SSL Policy Setting), geben Sie die SSL-Richtlinie in der Dropdown-Liste an, und klicken Sie auf OK, um die Richtlinie zu speichern.

Klicken **ASA FirePOWER-Änderungen speichern** um die Konfiguration der SSL-Richtlinie zu speichern.

Sie müssen die Zugriffskontrollrichtlinie bereitstellen. Bevor Sie die Richtlinie anwenden, sehen Sie eine veraltete Anzeige "Zugriffskontrollrichtlinie" auf dem Modul. Um die Änderungen am Sensor bereitzustellen, klicken Sie auf **Deploy** und wählen Sie die **Option Deploy FirePOWER Changes (FirePOWER-Änderungen bereitstellen).** Überprüfen Sie die vorgenommenen Änderungen, und klicken Sie im Popup-Fenster auf **Bereitstellen**.

Hinweis: Wenn Sie in Version 5.4.x die Zugriffsrichtlinie auf den Sensor anwenden möchten, klicken Sie auf **Apply ASA FirePOWER Changes**.

Hinweis: Navigieren Sie zu **Monitoring > ASA FirePOWER Monitoring > Task Status.** Anschließend beantragen Sie Konfigurationsänderungen, um sicherzustellen, dass die Aufgabe abgeschlossen ist.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

 Bei einer ausgehenden SSL-Verbindung fordert das System beim Durchsuchen einer öffentlichen SSL-Website aus dem internen Netzwerk eine Fehlermeldung für das Zertifikat an. Überprüfen Sie den Zertifikatsinhalt, und überprüfen Sie die CA-Informationen. Das interne Zertifizierungsstellenzertifikat, das Sie im FirePOWER-Modul konfiguriert haben, wird angezeigt. Akzeptieren Sie die Fehlermeldung zum Durchsuchen des SSL-Zertifikats. Um die Fehlermeldung zu vermeiden, fügen Sie das CA-Zertifikat in die Liste der vertrauenswürdigen CAs Ihres Browsers hinzu.

C Q Search

х

Certificate Viewer:"www.cisco.com"

<u>General</u> <u>D</u>etails

Could not verify this ce	rtificate because the issuer is unknown.
Issued To	
Common Name (CN)	www.cisco.com
Organization (O)	Cisco Systems
Organizational Unit (OU)	ATS
Serial Number	14:5E:8D:FB:06:DA:C6:55
Issued By	
Common Name (CN)	serverCA.example.com
Organization (O)	TAC
Organizational Unit (OU)	TAC
Period of Validity	
Begins On	Thursday, January 28, 2016
Expires On	Monday, January 29, 2018
Fingerprints	
SHA-256 Fingerprint	6C:66:D8:0E:52:5D:9D:D8:74:2F:A6:92:7F:31:E7:39: F2:E8:C7:B8:66:02:BC:A4:AF:F1:AB:92:56:B3:03:D7
SHA1 Fingerprint	9B:47:5B:E4:9D:2B:16:0D:FA:63:93:B1:53:F3:2D:6A:13:48:8E:ED

 Überprüfen Sie die Verbindungsereignisse, um zu überprüfen, welche SSL-Richtlinie und SSL-Regel vom Datenverkehr betroffen ist. Navigieren Sie zu Monitoring > ASA FirePOWER Monitoring > Real-Time Eventing.Wählen Sie eine Veranstaltung aus, und klicken Sie auf Details anzeigen. Überprüfen der SSL-Entschlüsselungsstatistik

Filter Connection Event Allow Im:: Wed 6/7/16 6:29:10 AM (IST) to Wed 6/7/16 6:29:14 ASA FirePOWER firewall connection event Reason: Reactive Fvent Details Triffic Initiator IP 192.168.20.50 / Responder IP 72.163.10.10 / Traffic G/7/16 Initiator IP 192.168.20.50 / Responder IP 72.163.10.10 / Traffic G/7/16 Initiator Country and not available Responder Country and not available Traffic Traffic G/7/16 Initiator Packets 9.0 Petination Port/ICMP 443 Petination Petination Petination Petination Petination Responder Country and not available Transchic Egress Interface Initiator G/7/16 Transection URL Category not available Dis Query not available G/7/16 Transection Application Risk unknown Piter Piter G/7/16 Policy Default Allow All Traffic Application Categories network protocols/services Sinbole Piter G/7/16 Policy Default Allow All Traffic Application Sis Leitent Sis Status Default	
Receiv Event Details Initiator Responder IP 72.163.10.10 // Traffic 6/7/16 Initiator Contry and not available Continent not available Ingress Security not available 6/7/16 Source Port/ICMP Type 56715 Destination Port/ICMP 443 Ingress Security not available 6/7/16 Source Port/ICMP Type 56715 Destination Port/ICMP 443 Ingress Interface inside 6/7/16 Transaction Initiator Packets 1.0 Intilator Packets 0 NetBIOS Domain not available 6/7/16 Initiator Bytes 752.0 Application Risk unknown HTTP Response DNS 6/7/16 Policy Default Allow All Traffic Client Application SL center SL Status Decrypt (Resign) 6/7/16 Friewall Policy Rule/SI Intrusion_detection Othour All Traffic Client Application SL protocol SSL Protocol 6/7/16 Policy Default Allow All Traffic Client Tag SSL protocol SSL Cipher Suite SSL Cipher Suite SSL Cipher Suite 6/7/16 Policy Default Allow All Tra	. AM (IST)
Receive Initiator Initiator Responder 72.163.10.10 Initiator 6/7/16 Initiator IP 192.168.20.50 Responder IP 72.163.10.10 Ingress Security not available 6/7/16 Initiator Country and not available not available Ingress Security not available 6/7/16 Source Port/ICMP Type 56715 Destination Port/ICMP 443 Ingress Interface inside 6/7/16 Initiator Packets 4.0 Initiator Packets 9.0 Initiator Packets 9.0 TOTP Flags 0 6/7/16 Initiator Packets 9.0 Not available TCP Flags 0 6/7/16 Initiator Packets 9.0 Not available TCP Flags 0 6/7/16 Initiator Packets 9.0 Not available TCP Flags 0 6/7/16 Initiator Packets 9.0 Not available TCP Flags 0 6/7/16 Initiator Packets 9.0 Application HTTP Response 0 6/7/16 Fores 752.0 Application Tag opens port Sinkhole not available 6/7/16 Policy Default Allow All Traffic Client Application SL client Version SSL client Version SSL Polic	
6/7/16Initiator IP192.168.20.50 / Initiator Country and not available ContinentResponder IP72.163.10.10 / 	
6/7/16 Initiator Country and Continent not available Continent not available Continent Initiator Country and Continent not available Continent Initiator Continent Initiator Continent Initiator Continent not available Continent Initiator Code	
6/7/16 Source Port/ICMP Type 56715 Destination Port/ICMP 443 Ingress Interface Ingress Inte	
6/7/16 User Special Identities/No Authentication Required URL https://cisco-tags.cisco.com/ Ingress Interface inside 6/7/16 Transaction URL https://cisco-tags.cisco.com/ Egress Interface outside 6/7/16 Initiator Packets 4.0 URL Reputation Risk unknown NetBIOS Domain not available 6/7/16 Initiator Packets 9.0 URL Reputation Risk unknown HTTP Response 0 6/7/16 Total Packets 13.0 Application HTTP S DNS Query not available 6/7/16 Responder Bytes 7486.0 Application Categories network protocols/services Sinkhole not available 6/7/16 Policy Default Allow All Traffic Client Application SSL client SSL status Decrypt (Resign) 6/7/16 Policy Default Allow All Traffic Client Categories web browser SSL policol 6/7/16 Policy Default Allow All Traffic Client Categories web browser SSL Policy 6/7/16 Policy Default Allow All Traffic Client Tag SSL protocol SSL Version 6/7/16 Monitor Rules not available Web Application Gisco SSL Clipher Suite <td></td>	
6/7/16 Transaction View Marking database with the part of t	
6/7/16 Transaction DRL Category Indext analysis C 6/7/16 Initiator Packets 4.0 URL Reputation Risk unknown Not BBIOS Domain not available 6/7/16 Initiator Packets 9.0 HTTP Response 0 DNS 6/7/16 Total Packets 13.0 Application HTTPS DNS Query not available 6/7/16 Responder Bytes 7486.0 Application Categories network protocols/services View more 6/7/16 Policy Default Allow All Traffic Client Application SSL client 6/7/16 Policy Default Allow All Traffic Client Categories web browser 6/7/16 Policy Default Allow All Traffic Client Categories web browser 6/7/16 Policy Default Allow All Traffic Client Tag SSL protocol 6/7/16 Nonitor Rules not available SSL Version SSL Version	
6/7/16 Initiator Packets 4.0 Not Replication Risk dining with the origination 6/7/16 Responder Packets 9.0 Initiator Packets 9.0 6/7/16 Total Packets 13.0 Application HTTPS DNS Query not available 6/7/16 Responder Bytes 752.0 Application HTTPS Sinkhole not available 6/7/16 Connection Bytes 7486.0 Application Categories network protocols/services View more 6/7/16 Policy Default Allow All Traffic Client Application SSL client SSL Policy 6/7/16 Policy Default Allow All Traffic Client Application not available SSL Policy 6/7/16 Policy Default Allow All Traffic Client Categories web browser SSL Policy 6/7/16 Policy Default Allow All Traffic Client Tag SSL protocol SSL Rule 6/7/16 Monitor Rules not available Gisco SSL Version TLS_0HE RSA_WITH_A	
of//10 Responder Packets 9.0 Intra Responder o DNS 6/7/16 Total Packets 13.0 Application HTTPS DNS Query not available 6/7/16 Total Packets 752.0 Application HTTPS Sinkhole not available 6/7/16 Responder Bytes 7486.0 Application Categories network protocols/services View more 6/7/16 Connection Bytes 8238.0 Application Tag opens port SsL 6/7/16 Policy Default Allow All Traffic Client Application SsL client SsL Policy 6/7/16 Policy Default Allow All Traffic Client Categories web browser SsL Policy Default SSL Policy 6/7/16 Policy Default Allow All Traffic Client Tag SsL protocol SsL Version TLS JDHE RSA_WITH_A 6/7/16 Monitor Rules not available Web Application Cisco SsL Version TLS JDHE RSA_WITH_A	
6/7/16	
6/7/16 Initiator Bytes 752.0 Application HTTPS Sinkhole not available 6/7/16 Responder Bytes 7486.0 Application Categories network protocols/services View more 6/7/16 Policy Application Tag opens port SSL Sinkhole not available 6/7/16 Policy Default Allow All Traffic Client Application SSL SSL SSL 6/7/16 Policy Default Allow All Traffic Client Categories web browser SSL Rule Outboound SSL Decrypt 6/7/16 Monitor Rules not available SSL View more SSL Policy 6/7/16 Policy Default Allow All Traffic Client Categories web browser SSL Rule Outboound SSL Decrypt 6/7/16 Monitor Rules not available Cisco SSL Version TLSv1.0	
6/7/16 Responder Bytes 7486.0 Application Categories network protocols/services View more 6/7/16 Connection Bytes 8238.0 Application Tag opens port SSL 6/7/16 Policy Default Allow All Traffic Client Application SSL client 6/7/16 Policy Default Allow All Traffic Client Version not available 6/7/16 Policy Default Allow All Traffic Client Categories web browser 6/7/16 Policy Default Allow All Traffic Client Tag SSL protocol 6/7/16 Monitor Rules not available Cisco SSL Version SSL Cipher Suite TLSv1.0 SSL Cipher Suite TLSv1.0	
6/7/16 Connection Bytes 8238.0 Application Tag opens port 6/7/16 Policy Client Application SSL client SSL Status Decrypt (Resign) 6/7/16 Policy Default Allow All Traffic Client Version not available SSL Status Decrypt (Resign) 6/7/16 Policy Default Allow All Traffic Client Categories web browser SSL Policy Default SSL Policy 6/7/16 Policy Rule/SI Intrusion_detection Client Tag SSL protocol SSL Version TLSv1.0 6/7/16 Nonitor Rules not available Web Application Cisco SSL Clipher Suite TLS DHE_RSA_WITH_A	
6/7/16 Policy Client Application SSL SSL 6/7/16 Policy Default Allow All Traffic Client Version not available SSL Status Decrypt (Resign) 6/7/16 Policy Default Allow All Traffic Client Version not available SSL Status Decrypt (Resign) 6/7/16 Policy Default Allow All Traffic Client Categories web browser SSL Rule Outboound SSL Decrypt 6/7/16 Monitor Rules not available Client Tag SSL protocol SSL Version TLSv1.0 SSL Version TLSv1.0 Web Application Cliso SSL Clipher Suite TLS DHE_RSA_WITH_A	
Policy Client Version not available SSL Status Decrypt (Resign) 6/7/16 Policy Default Allow All Traffic Client Version not available SSL Policy Default SSL Policy 6/7/16 Policy Default Allow All Traffic Client Categories web browser SSL Policy Default SSL Policy 6/7/16 Pirewall Policy Rule/SI Intrusion_detection Client Tag SSL protocol SSL Version TLSv1.0 Monitor Rules not available Web Application Cisco SSL Version TLSv1.0	
6/7/16 Policy Default Allow All Traffic Client Categories web browser SSL Policy Default SSL Policy 6/7/16 Firewall Policy Rule/S1 Intrusion_detection Client Tag SSL protocol SSL Rule Outboound_SSL Decryp 6/7/16 Monitor Rules not available Web Application Cisco SSL Version TLS JHE, RSA_WITH_A	
6/7/16 Firewall Policy Rule/SI Intrusion_detection Client Tag SSL protocol SSL Rule Outboound_SSL_Decryr. Monitor Rules not available Client Tag SSL protocol SSL Version TLSv1.0 Web Application Cisco SSL Clipher Suite TLS_DHE_RSA_WITH_A	
Monitor Rules not available Web Application Cisco SSL Version TLSv1.0 SSL Cipher Suite TLS_DHE_RSA_WITH_A	/pt
SSL Cipher Suite TLS_DHE_RSA_WITH_A	
6/7/16 Web App Categories web services provider SHA	AES_256_CBC
ISE Attributes Web App Tag SSL protocol SSL Certificate Valid	
6/7/16 End Point Profile Name not available Application Risk Medium Status	

- Stellen Sie sicher, dass die Bereitstellung der Zugriffskontrollrichtlinie erfolgreich abgeschlossen ist.
- Stellen Sie sicher, dass die SSL-Richtlinie in die Zugriffskontrollrichtlinie integriert ist.
- Stellen Sie sicher, dass die SSL-Richtlinie die entsprechenden Regeln für die eingehende und die ausgehende Richtung enthält.
- Stellen Sie sicher, dass SSL-Regeln die richtige Bedingung für die Definition des interessanten Datenverkehrs enthalten.
- Überwachen Sie die Verbindungsereignisse, um die SSL-Richtlinie und die SSL-Regel zu überprüfen.
- Überprüfen Sie den SSL-Entschlüsselungsstatus.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

<u>Technischer Support und Dokumentation - Cisco Systems</u>