Configuratie van de SSL decryptie op FirePOWER Module die ASDM (On-Box Management) gebruikt

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Uitgaande SSL-decryptie Inbound SSL-decryptie Configuratie voor SSL-decryptie Uitgaande SSL-decryptie (decrypt - Afgifte) Stap 1. Configuratie van het CA-certificaat. Stap 2. Het SSL-beleid configureren. Stap 3. Het beleid voor toegangscontrole configureren Inbound SSL-decryptie (decrypt - bekend) Stap 1. Importeer het servercertificaat en de -toets. Stap 2. Importeer het CA-certificaat (optioneel). Stap 3. Het SSL-beleid configureren. Stap 4. Configureer het toegangscontrolebeleid. Verifiëren Problemen oplossen Gerelateerde informatie

Inleiding

Dit document beschrijft de configuratie van Secure Socket Layer (SSL) decryptie op FirePOWER Module met behulp van ASDM (On-Box Management).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van ASA (adaptieve security applicatie) firewall, ASDM (adaptieve security applicatie Manager)
- Kennis van FirePOWER-apparaat
- Kennis van HTTPS/SSL-protocol

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASA FirePOWER-modules (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) met software versie 6.0.0 en hoger
- ASA FirePOWER-module (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) met software versie 6.0.0 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: Zorg ervoor dat FirePOWER Module een **Protect** licentie heeft om deze functionaliteit te configureren. Om de licentie te controleren dient u te navigeren naar **Configuration > ASA FirePOWER Configuration > Licentie**.

Achtergrondinformatie

Firepower Module decrypteert en inspecteert inkomende en uitgaande SSL verbindingen die naar deze worden omgeleid. Zodra het verkeer is gedecrypteerd, worden de getunnelde toepassingen zoals Facebookchat etc. gedetecteerd en gecontroleerd. De gecodeerde gegevens worden geïnspecteerd op bedreigingen, URL-filtering, bestandblokkering of kwaadaardige gegevens.

Uitgaande SSL-decryptie

De vuurkrachtmodule fungeert als de voorwaartse proxy voor uitgaande SSL-verbindingen door het onderscheppen van uitgaande SSL-verzoeken en het opnieuw genereren van een certificaat voor de site die de gebruiker wil bezoeken. De instantie van afgifte (CA) is het certificaat van zelfondertekening van vuurkracht. Als het certificaat van de vuurkracht geen deel uitmaakt van een hiërarchie die bestaat of als het niet wordt toegevoegd aan de browser cache van een klant, ontvangt de klant een waarschuwing terwijl hij doorbladert naar een beveiligde site. Decrypt-Resignatiemethode wordt gebruikt om uitgaande SSL decryptie uit te voeren.

Inbound SSL-decryptie

In het geval van inkomend verkeer naar een interne server of apparaat van het Web importeert de beheerder een kopie van het certificaat van de beschermde server en de sleutel. Wanneer het SSL servercertificaat op de vuurkrachtmodule wordt geladen, en het SSL decryptiebeleid wordt gevormd voor het inkomende verkeer, decrypteert het apparaat dan en inspecteert het verkeer wanneer het het verkeer door het verkeer leidt. De module detecteert dan kwaadaardige inhoud, bedreigingen, kwiek die over dit veilige kanaal stroomt. Bovendien wordt de Decrypt-Known Keymethode gebruikt om inkomende SSL decryptie uit te voeren.

Configuratie voor SSL-decryptie

Er zijn twee methoden van SSL-verkeersdecryptie.

- Decrypteren Aftreden voor Uitgaand SSL verkeer
- Decrypteren gekend voor Inbound SSL verkeer

Uitgaande SSL-decryptie (decrypt - Afgifte)

Firepower module fungeert als MITM (man-in-the-middle) voor SSL-onderhandelingen voor openbare SSL-servers. Het wijst het certificaat van de openbare server met een middelgroot CA certificaat af dat op de vuurkrachtmodule is ingesteld.

Dit zijn de drie stappen om de uitgaande SSL-decryptie te configureren.

Stap 1. Configuratie van het CA-certificaat.

Configureer een zelfgetekend certificaat of een middelmatig betrouwbaar CA-certificaat voor ontslag.

Het zelf-ondertekende CA-certificaat configureren

Om het CA-certificaat met eigen handtekening te configureren **navigeer** naar **Configuration > ASA Firepower Configuration > Objectbeheer > PKI > Interne CA's** en klik op **Generate CA**. Het systeem vraagt om informatie over het CA-certificaat. Zoals in de afbeelding wordt aangegeven, vult u de gegevens in zoals vereist.

Klik op **Generate zelfgetekende CA** om het interne CA certificaat te genereren. Klik vervolgens op **Generate CSR** om het certificaat-teken-verzoek te genereren dat dientengevolge met de CA

server wordt gedeeld om te tekenen.

Het middelste CA-certificaat configureren

Om het Intermediate CA Certificaat te configureren dat door een andere derde CA wordt ondertekend, navigeer naar Configuratie > ASA Firepower Configuration > Objectbeheer > PKI > Interne CA's en klik op Importeren CA.

Specificeer de naam van het certificaat. Selecteer de optie Bladeren en uploaden het certificaat vanuit de lokale machine of kopieer de inhoud van het certificaat in de optie **certificaatgegevens**. Om de privétoets van het certificaat te specificeren, bladert u door het sleutelbestand of kopieert u de toets in de optie **Key**.

Als de toets is versleuteld, stelt u het vakje **Encrypted** in en specificeert u het wachtwoord. Klik op **OK** om de certificaatinhoud op te slaan, zoals in de afbeelding wordt weergegeven:

Configuration > ASA FirePOWE	<u>R Configuration > Object Management</u> > <u>PKI</u> > <u>Internal CAs</u>	
ASA FirePOWER Configuration 🗉		
	Constante CA	(Import CA
Port	U Ocietate CA	Import CA
Security Zones	Import Internal Certificate Authority	? ×
	Name: Intermediate-CA	
	Interneulate-CA	
Variable Set	Certificate Data or, choose a file: Browse	
Sinkhole	CBMCS0ExEjAQBaNVBAcTCUJBTkdBTE9SRTE0MAwGA1UEChMF00IT008xDDAKBaNV	
📝 FileList 😑	BASTA1RBQzEaMBgGA1UEAxMRQ0Euc2VydmVydGVzdC5jb20xIzAhBgkqhkiG9w0B	
Cipher Suite List	CQEWFGFkbWluQHNlcnZlcnRlc3QuY29tggkA9OflOUfXIF0wDAYDVR0TBAUwAwEB	
🕀 🚽 Distinguished Name	Y24NBgKthKiG9W0BAQ0FAA0BgQCXQME242l0SKT2ghQt5HuNWQF/NQK32S5JUVF YY24RJinUUiW5mC4lD1KSvG+1x26OlbWRs4vwfl8En3Dct0kRa74OnOr7S8l83E9	
PKI	kuIpr+e7T+QifHbG4AzF5b2WGF4HUCxXjYTKtVHwbLuNeED5cAB38jL7Vso0cvg2	
Trusted CAs	Biat1w==	
External Certs	END CERTIFICATE	
- 😝 Internal Certs		
	Key or, choose a file: Browse	
	i/DpuPr0S2LiaDpN2xShcuMTaRN+1xMOTInfTpar/0LpM/AEapSizAEAcTzNmA4aP/	
Internal Cert Groups	3XMIL1RbCFUpUvL9D2N+4TuZzHrbmUa6OA1gPNvLcf0Vf1wgVvagZYYAn5oA50wA	
Evternal Cert Groups III	K554gAeIvYJC5dEXe9974K9nh7/hNG5B53S3gKuGGvQx+0DSilZy0J0RPzRnQmew	
	cNsbTQ3TGcdt6p58cJFsTWYZayvvQCbeJHOgNcGOUcfdlZ2/v6IoVC0wp+61KgZ7	
A Device Setup	JIGYPDSKZJJSAX9BKKFXDSSAFJ3DSZ9ZtX/JFIVaM0JEUQQCtEPP69FaV6Z50TD0 wFkMModEPeSBol7WLTiKuivRLM0/n7DsM41Wdn4x112i2k+E9AWoXw+kGE9PwNBO	
	22WYRn92UiZWTKySdU0Mr4mDRVBkzb+Iqb30D7/S7ENWFpuktxWOQA==	
Firewaii	END RSA PRIVATE KEY	-
Remote Access VPN	Encrypted and the paceword ic:	
Site-to-Site VPN		
ASA FirePOWER Configuration	ок	Cancel

Stap 2. Het SSL-beleid configureren.

SSL-beleid definieert de decryptie-actie en identificeert het verkeer waarop de decryptieafgiftemethode wordt toegepast. Configureer de meerdere SSL-regels op basis van uw zakelijke vereisten en het beveiligingsbeleid van de organisatie.

Om het SSL beleid te configureren **navigeer** om **> ASA FirePOWER Configuration > Policy > SSL** te **configureren** en op **Add Rule** te klikken.

Naam: Specificeer de naam van de regel.

Actie: Specificeer de actie als decrypt - ontvang en kies het CA certificaat van de vervolgkeuzelijst

die in de vorige stap is ingesteld.

Bepaal de voorwaarden in de regel om verkeer aan te passen zoals er meerdere opties zijn (zone, netwerk, gebruikers enz.), gespecificeerd om het verkeer te definiëren dat moet worden gedecrypteerd.

Om de gebeurtenissen van SSL decryptie te genereren, schakelt u de logingat **logging** optie in zoals in de afbeelding:

O O ASA FirePOWER Configurat	○ ○ ○ <u>Configuration > ASA Fi</u>	rePOWER Configuration > Policies	> <u>SSL</u>		
V Dolicies					
🚦 Access Control Policy	Default SSL Policy				
Intrusion Policy					
🖺 Files	SSL POICY				
SSL					
🔯 Actions Alerts					
🚨 Identity Policy	Rules Trusted CA Certificates	Undecryptable Actions			
DNS Policy				Add Category (3) Add Rule Search Rules	
🕨 🌄 Device Management					~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
🕨 🧐 Object Management	Add Bule				? X
► 🏠 Local					
System Information	Name Outboound SSI Decrypt	1	Enabled	Insert into Category	andard Pules
I Updates					
Licenses	Action 🔂 Decrypt - Resign	 with ServerCA 	▼ C	Replace Key	
ritegration	Zones Networks Use	rs Applications Ports Categor	Certificate DN Cert Status	S Cipher Suite Version	Logging
	Available Networks		Source Networks (1)	Destination Networks (0)	
	Search by name or value		Private Networks	any any	
	Networks	Geolocation			
		Colocation			
	Private Networks	Add to			
		Source			
		Destination			
A Device Setup			Enter an IP address	Add Enter an IP address	Add
Firewall					Add Cancel
🥂 <u>R</u> emote Access VPN					
				No data to display	A Page 1 of 1 N M
ASA FirePOWER Configur					rage 1 OI 1 7 7 C
~					

Klik op Add om de SSL-regel toe te voegen.

Klik op Store ASA Firepower Wijzigingen om de configuratie van SSL beleid op te slaan.

Stap 3. Het beleid voor toegangscontrole configureren

Zodra u het SSL beleid met de juiste regels vormt, moet u het SSL beleid in het Toegangsbeheer specificeren om de veranderingen uit te voeren.

Om het beleid voor toegangscontrole te configureren **navigeer** naar **Configuratie > ASA Firepower Configuration > Policy > Access Control.**

Klik of op **Geen** van het **SSL Beleid** of navigeer naar **Geavanceerd > SSL Policy Setting**. Specificeer het SSL-beleid in de vervolgkeuzelijst en klik op **OK** om het op te slaan, zoals in de afbeelding:

O O ASA FirePOWER Configurat	O O O Configuration > ASA FirePOWER Configuration > Policies > Access C	<u>ontrol</u>
▼		
Access Control Policy	ASA ASA FirePOWER	
▶		_
🖹 Files	Default Allow All Traffic	
🔒 SSL		
🔋 Actions Alerts	Enter a description	
🚨 Identity Policy		
DNS Policy		
🕨 🐻 Device Management		
🕨 🧒 Object Management		
🕨 🏠 Local	Identity Policy: None SSL Policy: None	
ன System Information		
📑 Updates	Rules Security Intelligence HTTP Responses Advanced	
Licenses	General Settings	Ø
Tools		
Integration	Maximum URL characters to store in connection events	1024
	Allow an Interactive Block to bypass blocking for (seconds)	600
	Retry U SSI Policy to use for inspecting encrypted ? X	Yes
	connections	Mark
	Inspect	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

Klik ASA FireSIGHT-wijzigingen opslaan om de configuratie van SSL beleid op te slaan.

Je moet het toegangscontrolemiddel op de sensor zetten. Voordat u het beleid toepast, is er een indicatie dat **Access Control Policy verouderd is** op de module. Om de wijzigingen in de sensor in te stellen, klikt u op **Importeren** en selecteert u **optie FirePOWER Wijzigingen implementeren**. Controleer de aangebrachte wijzigingen en klik op **Importeren**.

Opmerking: In versie 5.4.x, als u het toegangsbeleid op de sensor moet toepassen, klik op ASA FirePOWER Wijzigingen toepassen.

Opmerking: Navigeer naar **bewaking > ASA FirePOWER Monitoring > Taakstatus.** U dient vervolgens wijzigingen in de configuratie in om er zeker van te zijn dat de taak is voltooid.

Inbound SSL-decryptie (decrypt - bekend)

De inkomende SSL Decryptie (Decrypt-Known) methode wordt gebruikt om het inkomende SSL verkeer te decrypteren waarvoor u het servercertificaat en de privé sleutel hebt gevormd. U moet het servercertificaat en de privétoets naar de FirePOWER-module importeren. Wanneer SSL-verkeer de Firepower module raakt, ontsleutelt het het verkeer en voert het de inspectie uit op gedecrypteerd verkeer. Na inspectie, herversleutelt de Firepower module het verkeer en verstuurt het naar de server.

Dit zijn de vier stappen om de uitgaande SSL-decryptie te configureren:

Stap 1. Importeer het servercertificaat en de -toets.

Als u het servercertificaat en de -toets wilt importeren, navigeer dan naar **configuratie > ASA Firepower Configuration > Objectbeheer > PKI > Interne Certs** en klik op **Add Internal Cert**.

Specificeer zoals in de afbeelding de naam van het certificaat. Selecteer ofwel browsen om het certificaat uit de lokale machine te selecteren of kopieer de inhoud van het certificaat in de **certificaatgegevens**. Om de privétoets van het certificaat te specificeren, bladert u door het sleutelbestand of kopieert u de toets in de optie-**toets**.

Als de toets is versleuteld, schakelt u het **versleutelde** keuzevakje in en specificeert u het wachtwoord, zoals in de afbeelding:

O O ASA FirePOWER Configurat	• • • • • • • • • • • • • • • • • • •
Application Filters	
► WRL	Add Internal Cast
GeoLocation	
🔦 Variable Set	Na Add Known Internal Certificate ? ×
SecurityIntelligence	
Sinkhole	Name: web.servertest.com
📝 FileList	
🔅 Cipher Suite List	Certificate Data or, choose a file: Browse
🕨 🗳 Distinguished Name	nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA0ucjKK9ofSyrAbYkSKC/nvy2g7Mj
🔻 🔦 РКІ	RHbV0UEK+2a5u5fDvZIRURHHBEbFp+SV0E7ak7PljdXd/sB4nhvvfPe4FN65IurN
🖶 Internal CAs	mj2ryw0y42l8u520r/9rnNJo2/212avR4u21PA9AQqXvyeCCL/0CQmFQ0rP6+qbk +FPHLf9wFxBahpECAwEAATANBakahkiG9w0BAOsFAAOBaOCukZVPuTaiJeuiPrtF
🖶 Trusted CAs	Lrcyns+lrbHTJhge0Z2HC/XJmYwyJXhBuEqvU9qx+GhQ99jNCOlo0iPIGF1naqBt
🖶 External Certs	FtI7ohmI/F544x75fm17t3XwfZF/VA2GhG3W3QGFKHCA0U7CBaU78jCVBa9CTKOG
🖶 Internal Certs	END CERTIFICATE
👶 Internal CA Groups	
👶 Trusted CA Groups	
👶 Internal Cert Group:	key or, choose a file: browse
🐣 External Cert Group	
🕨 🏠 Local	EccERsWn5JXOTtoTs+WN1d3+wHieG+9897aU3rki6s2aPNiLBTLiOLv5LM6v/1iE
ன System Information	0mjP/YjZ29Hi5nU8D0BCpe/J4IIv84JCYVA6s/r6puT4U8ct/3AXEGCGkQIDAQAB
📑 Updates	AoGBAJ+XOAu5cCAIhP6ujZZHzbjJEnNmQvGz2uiVh3HlsfY6SWxR87ic8zRROZBq
🔛 Licenses	+nzEJwx4LgmXR8N88YbkvC3n4iVY5z90fsvCdJ2UoAGBXN4BAkEA+nkDe1UglxOz
🔻 💼 Tools	Pgmzad68lngk4/7Wbg8ibZz0Mv2PSvO7pNbhRfpy/dtgGLJvIGJIr/+0iL2SrPFv
🗑 Backup Restore	d7QmDkGwyQJBANeOlVWWjBPuFCLQjYL04c66km9vzGgLDHjGc4gOING1iFlCrQt1
Cehaduling	Encrypted, and the password is:
💑 <u>D</u> evice Setup	Store ASA FirePOWER Changes Cancel

Klik op Store ASA FirePOWER Wijzigingen om de certificaatinhoud op te slaan.

Stap 2. Importeer het CA-certificaat (optioneel).

Voor een servercertificaat dat is getekend door een interne tussenpersoon of een basiscertificaat, moet u de interne keten CA-certificaten importeren naar de vuurkrachtmodule. Nadat de invoer is uitgevoerd, kan de vuurkrachtmodule het servercertificaat valideren.

Als u het CA-certificaat wilt importeren, navigeer dan naar **Configuratie > ASA Firepower Configuration > Objectbeheer > Trusted CA's** en klik op **Add Trusted CA** om het CA-certificaat toe te voegen.

Stap 3. Het SSL-beleid configureren.

SSL beleid definieert de actie- en serverdetails waarvoor u de decrypt-bekende methode wilt configureren om het inkomende verkeer te decrypteren. Als u meerdere interne servers hebt, moet u meerdere SSL-regels configureren op basis van verschillende servers en het verkeer dat zij verwerken.

Om het SSL beleid te configureren **navigeer** om **> ASA FirePOWER Configuration > Policy > SSL** te **configureren** en op **Add Rule** te klikken.

Naam: Specificeer de naam van de regel.

Actie: Specificeer de actie als **Decrypt - bekend** en kies het CA certificaat uit de vervolgkeuzelijst die in de vorige stap is ingesteld.

Defineer de voorwaarde om deze regels aan te passen, aangezien er meerdere opties (netwerk, toepassing, poorten enz.) zijn gespecificeerd om het interessante verkeer van de server te definiëren waarvoor u de SSL decryptie wilt inschakelen. Specificeer de interne CA in **Geselecteerde Trusted CAs in** tabblad **Trusted CA certificaat**.

Om de gebeurtenissen van SSL decryptie te genereren, schakelt u de logingat logging optie in.

○ ○ ○ ASA FirePOWER Configurat	○ ○ ○ <u>Con</u>	figuration > .	ASA Fire	POWER Config	uration	> Policies >	<u>SSL</u>								
Policies Policies Access Control Policy © Intrusion Policy © Intrusion Policy Frue Editor	Defaul SSL Policy	t SSL Pol	licy												26 12
 Files SSL Actions Alerts 	Rules	rusted CA Cert	ificates	Undecryptabl	e Actions	-				0					
Lentity Policy	Add Rule														? ×
Bovice Management Object Management	Name W	eb_Server_Decr	ypt				Enabled	đ	Ir	nsert be	low rule		▼ 1		
 Vision Strategy (Section 1997) Network 	Action 🔒	Decrypt - Knov	vn Key	✓ with	web.serve	rtest.com			Edit						
Port Security Zones	Zones	Networks	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Cipher	Suite	Version			Logging
P Application Filters	Available I	Networks 🖒					Source Netwo	orks (0)			Destina	ation Networks	(1)	
VRL	🔍 Search	by name or valu	le				any					👳 192	2.168.10.5/32		
GeoLocation	N	etworks		Geolocation											
 [™] SecurityIntelligence [™] Sinkhole [™] FileList [™] Cipher Suite List [™] Distinguished Name [♥] Q. PKI [♥] Internal CAs [♥] Trusted CAs [♥] External Certs [●] 	Private	Networks				Add to Source Add to Destination	Foter an IP a	Idress			Δdd	Enter a	n IP address		Add
							Enter an IP ad	adress			Add	Enter a	in IP address	Add	Cancel
🚱 es - 11															

Klik op Add om de SSL-regel toe te voegen.

Klik vervolgens op **Store ASA Firepower Wijzigingen** om de configuratie van SSL beleid op te slaan.

Stap 4. Configureer het toegangscontrolebeleid.

Zodra u het SSL beleid met de juiste regels vormt, moet u het SSL beleid in het Toegangsbeheer specificeren om de veranderingen uit te voeren.

Om het beleid voor toegangscontrole te configureren **navigeer** naar **Configuratie > ASA Firepower Configuration > Policy > Access Control.**

Klik op de optie **Geen** naast **SSL Policy** of navigeer naar **Advanced > SSL Policy Setting**, specificeer het SSL-beleid in de vervolgkeuzelijst en klik op **OK** om het op te slaan.

Klik ASA FireSIGHT-wijzigingen opslaan om de configuratie van SSL beleid op te slaan.

U moet het beleid voor toegangscontrole implementeren. Voordat u het beleid toepast, kunt u een indicatie Toegangsbeleid op de module zien. Om de veranderingen in de sensor in te zetten, klikt u op **Uitvoeren** en kiest u **optie FirePOWER Veranderingen implementeren.** Controleer de aangebrachte wijzigingen en klik op In het pop-upvenster **implementeren**.

Opmerking: In versie 5.4.x, als u het toegangsbeleid op de sensor moet toepassen, klik op **ASA FirePOWER Wijzigingen toepassen**.

Opmerking: Navigeer naar **bewaking > ASA FirePOWER Monitoring > Taakstatus.** U dient vervolgens wijzigingen in de configuratie in om er zeker van te zijn dat de taak is voltooid.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

 Voor een uitgaande SSL-verbinding maakt het systeem, nadat u door een openbare SSLwebsite van het interne netwerk bladert, een foutmelding van het certificaat. Controleer de certificaatinhoud en controleer de CA-informatie. Het interne CA-certificaat dat u in de FirePOWER-module hebt ingesteld, wordt weergegeven. Neem de foutmelding in om door het SSL-certificaat te bladeren. Om de foutmelding te voorkomen, voegt u het CA-certificaat toe aan de vertrouwde CA-lijst van uw browser.

х

Certificate Viewer:"www.cisco.com"

General Details

Could not verify this co	ertificate because the issuer is unknown.
Issued To	
Common Name (CN)	www.cisco.com
Organization (O)	Cisco Systems
Organizational Unit (OU	I) 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	J) 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

 Controleer de verbindingsgebeurtenissen om te verifiëren welk SSL beleid en SSL regel door het verkeer zijn verbonden. Navigeer naar bewaking > ASA FirePOWER-bewaking > Real-Time Eventing.Selecteer een gebeurtenis en klik op View Details. Controleer de SSLdecryptie statistieken.

	FirePOWER Events Connecti	on Intrusion File Malwa	re File Security Intelligence			
Filter	Connection Event Allo ASA FirePOWER firewall connec Reason:	tion event		Time: Wed 6/7/16 6:	29:10 AM (IST) to	Wed 6/7/16 6:29:11 AM (IST)
👂 Re	Event Details					
Receiv	Initiator		Responder		Traffic	
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 Continent	not available	Responder Country and Continent	not available	Zone Egress Security	not available
	Source Port/ICMP Type	56715	Destination Port/ICMP	443	Zone	insido
6/7/16	User	Special Identities/No Authentication Required	URL	https://sicco.togs.cicco.com	Egress Interface	outside
		Autoritedulor required		nups://cisco-tags.cisco.com /	TCP Flags	0
6///16	Transaction			Risk unknown	NetBIOS Domain	not available
6/7/16	Initiator Packets	4.0	HTTP Response	0		
0,7,10	Responder Packets	9.0		•	DNS	
6/7/16	Total Packets	13.0	Application		DNS Query	not available
	Initiator Bytes	752.0	Application	HTTPS	Sinkhole	not available
6/7/16	Responder Bytes	7486.0	Application Categories	network protocols/services	View more	
	Connection Bytes	8238.0	Application Tag	opens port		
6/7/16			Client Application	SSL client	SSL	
	Policy		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
CITIL	Firewall Policy Rule/SI	Intrusion_detection	Client Tag	SSL protocol	SSL Rule	Outboound_SSL_Decrypt
6/7/16	Monitor Pulos	not susilable	Web Application	Cisco	SSL Version	TLSv1.0
6/7/16	Monitor Rules	nut available	Web App Categories	web services provider	SSL Cipher Suite	TLS_DHE_RSA_WITH_AES_256_CB SHA
.,.,	ISE Attributes		Web App Tag	SSL protocol	SSL Certificate	Valid
6/7/16	End Point Profile Name	not available	Application Risk	Medium	Status	
	Security Group Tag	not available	Application Business	Medium	SSL Flow Error	Success

- Zorg ervoor dat de implementatie van het toegangsbeheerbeleid is voltooid.
- Zorg ervoor dat het SSL-beleid in het toegangsbeleid is opgenomen.
- Zorg ervoor dat SSL-beleid passende regels voor inkomende en uitgaande richting bevat.
- Zorg ervoor dat SSL-regels de juiste voorwaarde bevatten om het interessante verkeer te definiëren.
- Controleer de verbindingsgebeurtenissen om het SSL beleid en de SSL regel te verifiëren.
- Controleer de SSL-decryptie status.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

• Technische ondersteuning en documentatie - Cisco Systems