Configurazione della decrittografia SSL sul modulo FirePOWER utilizzando ASDM (gestione integrata)

Sommario

Introduzione Prerequisiti **Requisiti** Componenti usati Premesse Decrittografia SSL in uscita Decrittografia SSL in ingresso Configurazione per la decrittografia SSL Decrittografia SSL in uscita (Decrittografia - Abbandona) Passaggio 1. Configurare il certificato CA. Passaggio 2. Configurare il criterio SSL. Passaggio 3. Configurare i criteri di controllo di accesso Decrittografia SSL in ingresso (decrittografia - nota) Passaggio 1. Importare il certificato e la chiave del server. Passaggio 2. Importare il certificato CA (facoltativo). Passaggio 3. Configurare il criterio SSL. Passaggio 4. Configurare i criteri di controllo di accesso. Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene descritta la configurazione della decrittografia SSL (Secure Sockets Layer) sul modulo FirePOWER con ASDM (On-Box Management).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza del firewall ASA (Adaptive Security Appliance), ASDM (Adaptive Security Device Manager)
- Conoscenza dell'appliance FirePOWER
- Conoscenza del protocollo HTTPS/SSL

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Moduli ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) con software versione 6.0.0 e successive
- Modulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) con software versione 6.0.0 e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Nota: Verificare che il modulo FirePOWER disponga di una licenza **Protect** per configurare questa funzionalità. Per verificare la licenza, selezionare **Configurazione > ASA FirePOWER Configuration > Licenza**.

Premesse

Il modulo Firepower decrittografa e controlla le connessioni SSL in entrata e in uscita a esso reindirizzate. Una volta che il traffico è decriptato, le applicazioni tunneling come Facebook chat ecc, vengono rilevate e controllate. I dati decrittografati vengono ispezionati alla ricerca di minacce, filtri URL, blocchi di file o dati dannosi.

Decrittografia SSL in uscita

Il modulo firepower funge da proxy di inoltro per le connessioni SSL in uscita intercettando le richieste SSL in uscita e rigenerando un certificato per il sito che l'utente desidera visitare. L'autorità emittente è il certificato autofirmato Firepower. Se il certificato di firepower non fa parte di una gerarchia esistente o se non viene aggiunto alla cache del browser di un client, il client riceve un avviso mentre accede a un sito protetto. Il metodo Decrypt-Resignmethod viene utilizzato per eseguire la decrittografia SSL in uscita.

Decrittografia SSL in ingresso

In caso di traffico in entrata verso un server Web o un dispositivo interno, l'amministratore importa una copia del certificato del server protetto e la chiave. Quando il certificato server SSL viene caricato sul modulo firepower e i criteri di decrittografia SSL sono configurati per il traffico in entrata, il dispositivo decrittografa e controlla il traffico mentre inoltra il traffico. Il modulo rileva quindi contenuti dannosi, minacce e malware che passano attraverso questo canale sicuro. Inoltre, il metodo Decrypt-Known Keymethod viene utilizzato per eseguire la decrittografia SSL in ingresso.

Configurazione per la decrittografia SSL

Esistono due metodi per decrittografare il traffico SSL.

- Decrittografa Abbandona per traffico SSL in uscita
- Decrittografa Noto per il traffico SSL in entrata

Decrittografia SSL in uscita (Decrittografia - Abbandona)

Il modulo Firepower agisce come MITM (man-in-the-middle) per qualsiasi negoziazione SSL per i server SSL pubblici. Rinuncia al certificato del server pubblico con un certificato CA intermedio configurato nel modulo firepower.

Di seguito vengono riportati i tre passaggi per configurare la decrittografia SSL in uscita.

Passaggio 1. Configurare il certificato CA.

Configurare un certificato autofirmato o un certificato intermedio di una CA attendibile per la revoca del certificato.

Configurare il certificato CA autofirmato

Per configurare il certificato CA autofirmato, selezionare **Configurazione > Configurazione ASA Firepower > Gestione oggetti > PKI > CA interne** e fare clic su **Genera CA**. Il sistema richiede i dettagli del certificato CA. Come mostrato nell'immagine, compilare i dettagli in base alle proprie esigenze.

ASA FirePOWER Configur 🗗 👎	Configuration > ASA FirePOWER Configuration > Ob	ject Management > <u>PKI</u> > <u>Internal CAs</u>
Opject nanogement Opject nanogement	Name	Generate CA Import CA
With the set of the sec of t	Generate Internal Certific	ServerCA
FileList Gipher Suite List Gipher Suite List Gifter Suite List Gif	Country Name (two-letter cod State or Province: Locality or City:	KA Bangalore
···· 🖶 Trusted CAs ···· 🖶 External Certs ···· 🖶 Internal Certs ···· 🐥 Internal CA Groups ···· 🖧 Trusted CA Groups	Organization: Organizational Unit (Departme Common Name:	ent): TAC serverCA.example.com
Internal Cert Groups External Cert Groups Local		
	Generate CSR	Generate self-signed CA Cancel
Site-to-Site VPN		

Fare clic su **Genera CA autofirmata** per generare il certificato CA interno. Fare quindi clic su **Generate CSR** per generare la richiesta di firma del certificato, che viene quindi condivisa con il

server CA per la firma.

Configurare il certificato CA intermedio

Per configurare il certificato CA intermedio firmato da un'altra CA di terze parti, selezionare Configurazione > ASA Firepower Configuration > Object Management > PKI > CA interne e fare clic su Importa CA.

Specificare il nome del certificato. Selezionare **Sfoglia** e carica il certificato dal computer locale oppure copiare e incollare il contenuto del certificato nell'opzione **Dati certificato**. Per specificare la chiave privata del certificato, sfogliare il file di chiave o copiare e incollare la chiave nell'opzione **Key**.

Se la chiave è crittografata, selezionare la casella di controllo **Crittografato** e specificare la password. Fare clic su **OK** per salvare il contenuto del certificato, come mostrato nell'immagine:

Configuration > ASA FirePOWE	R Configuration > Object Management > PKI > Internal CAs	
ASA FirePOWER Configuration		
Operation of the sector o	Generate CA	Import CA
Port Port	Import Internal Certificate Authority Name: Intermediate-CA Certificate Data or, choose a file: Browse CBMCS0ExEjAQBgNVBAcTCUJBTkdBTE9SRTEOMAwGA1UEChMFQ0ITQ08xDDAKBgNV BASTA1RBQzEaMBgGA1UEAxMRQ0Euc2VydmVydGVzdC5jb20xIzAhBgkqhkiG9w0B CQEWFGFkbWluQHNIcnZlcnRlc3QuY29tggkA9OflOUfXIF0wDAYDVR0TBAUwAwEB /zANBgkqhkiG9w0BAQUFAAOBgQCXQME24zt0sKTzghQI5HuNWQl7NQK3Z55juVF YY24BJinUUiW5mCAID1KSyG+Jx26QlbWRs4vwfl8Fq3Dct0kRg74Qp0zZS8l83F9 kuIpr+e7T+QifHbG4AzF5b2WGF4HUCxXjYTKtVHwbLuNeED5cAB38jL7Vso0cvg2 Biat1w== END CERTIFICATE	? ×
Internal Certs	Key or, choose a file: i/DnuBs9S3UgPnN3xShcwMTg8N+1yWOTJnfIpar/0LpW4Eqn5izAEAcTzNmA4gR/ 3XMII 18hCEI Ini Ivi 9D2N+4Tu7zHrbmUa6OA1gPNwi cf0Vf1wgAvag7XXAp5oA50wA	•
Evternal Cert Groune III Device Setup	K554gAeItV1JC5dEXe9974K9nh7/hNG5B53S3gKuGGvQx+dDSilZy0J0RPzRnQmew cNsbTQ3TGcdt6p58cJFsTWYZayvvQCbeJHOgNcGOUcfdlZ2/v6IoVC0wp+61KgZ7 jIgYPD5KzjJ5AX9BRKFXbsSAFJ3bSZ9Ztx/jFlvaMdjEUqqctEPP69Fav6z5dTDo wFkMModFPe5Bol7WLTjKujyRLM0/p7bsM41Wdn4x1J2j2k+E9AWoXw+kGF9PwNBQ 23WVPp02U/20WTkv5dU0Md4mDPV/RkfbvLidb2D2/CZ5DWVFpuktryWOQA = =	
Firewall	END RSA PRIVATE KEY	
Remote Access VPN	Encrypted, and the password is:	
ASA FirePOWER Configuration	ОК	Cancel

Passaggio 2. Configurare il criterio SSL.

Il criterio SSL definisce l'azione di decrittografia e identifica il traffico su cui viene applicato il metodo di decrittografia Decrypt-Resign. Configurare le regole SSL multiple in base ai requisiti aziendali e ai criteri di sicurezza dell'organizzazione.

Per configurare il criterio SSL, selezionare **Configure > ASA FirePOWER Configuration > Policies > SSL** (Configurazione ASA FirePOWER > Criteri > SSL), quindi fare clic su **Add Rule** (Aggiungi regola).

Nome: specificare il nome della regola.

Azione: specificare l'azione come **Decrittografa - Abbandona** e scegliere il certificato CA dall'elenco a discesa configurato nel passaggio precedente.

Definire le condizioni nella regola per far corrispondere il traffico in quanto sono disponibili più opzioni (zona, rete, utenti e così via), specificate per definire il traffico da decrittografare.

Per generare gli eventi di decrittografia SSL, abilitare l'opzione di **registrazione** all**'accesso**, come mostrato nell'immagine:

O O ASA FirePOWER Configurat	O O Configuration > ASA FirePOWER Configuration > Policies > SSL	
V Dolicies		
Access Control Policy	Default SSL Policy	
Intrusion Policy		
🖻 Files	SSL Policy	
🔒 SSL		
🔯 Actions Alerts	N I	
🚨 Identity Policy	Rules Trusted CA Certificates Undecryptable Actions	
DNS Policy	Add Coheney Add Bule Search Buler	~
🕨 📕 Device Management	Add Category Add Category Add Category Add Category Add Category	~
🕨 🧒 Object Management	Add Pulo	_
🕨 🏠 Local	Adu kule	`
System Information		
📑 Updates	Name Outboound_SSL_Decrypt	
Licenses	Action 🛗 Decrypt - Resign 🗸 with ServerCA 🗸 C 🖸 Replace Key	
Tools		
🕨 🔩 Integration	Zones Networks Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Logging	
	Available Networks 🏷 🙆 Source Networks (1) Destination Networks (0)	
	Search by name or value	
	Networks Geolocation	
	Private Networks	
	Add to	
	Source	
	Add to	
	Destination	
Bevice Setup	Enter an IP address Add Enter an IP address Add	
Firewall		
	Alu Calica	_
Kemote Access VPN		
Site-to-Site VPN		
	No data to display 🔣 🐇 Page 1 🛛 of 1 为 💓 🖉	;
ASA FirePOWER Configur		

Fare clic su Add per aggiungere la regola SSL.

Fare clic su Store ASA Firepower Changes per salvare la configurazione del criterio SSL.

Passaggio 3. Configurare i criteri di controllo di accesso

Dopo aver configurato il criterio SSL con le regole appropriate, è necessario specificare il criterio SSL nel controllo di accesso per implementare le modifiche.

Per configurare il criterio di controllo dell'accesso, selezionare **Configurazione > Configurazione di** ASA Firepower > Criteri > Controllo dell'accesso.

Fare clic su **None** (Nessun criterio **SSL**) oppure selezionare **Advanced** (Avanzate) > **SSL Policy Setting** (Impostazione criterio SSL). Specificare il criterio SSL dall'elenco a discesa e fare clic su OK per salvarlo, come mostrato nell'immagine:

O O ASA FirePOWER Configurat	Configuration > ASA FirePOWER Configuration > Policies > Access C	ontrol I
▼		
E Access Control Policy	ASA ASA FirePOWER	
Intrusion Policy		
💾 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 SSL Policy to use for inspecting encrypted ? ×	Yes
	connections	Vac
	Inspect	Tes
	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

Clic Archivia modifiche ASA Firepower per salvare la configurazione del criterio SSL.

Ènecessario distribuire i criteri di controllo di accesso al sensore. Prima di applicare il criterio, è possibile che i **criteri di controllo di accesso non siano aggiornati** sul modulo. Per distribuire le modifiche al sensore, fare clic su **Distribuisci** e selezionare l'opzione **Distribuisci modifiche FirePOWER. Verificare le modifiche apportate e fare clic su Distribuisci.**

Nota: Nella versione 5.4.x, se è necessario applicare la policy di accesso al sensore, fare clic su **Apply ASA FirePOWER Changes** (Applica modifiche FirePOWER ASA).

Nota: Selezionare Monitoraggio > Monitoraggio di ASA Firepower > Stato task. È quindi necessario richiedere le modifiche alla configurazione per assicurarsi che l'attività sia stata completata.

Decrittografia SSL in ingresso (decrittografia - nota)

Il metodo Decrittografia SSL in entrata (Decrypt-Known) viene utilizzato per decrittografare il traffico SSL in entrata per il quale sono stati configurati il certificato server e la chiave privata. È necessario importare il certificato del server e la chiave privata nel modulo Firepower. Quando il traffico SSL colpisce il modulo Firepower, lo decrittografa ed esegue l'ispezione sul traffico decrittografato. Dopo l'ispezione, il modulo Firepower crittografa nuovamente il traffico e lo invia al server.

Di seguito vengono riportati i quattro passaggi per configurare la decrittografia SSL in uscita:

Passaggio 1. Importare il certificato e la chiave del server.

Per importare il certificato e la chiave del server, selezionare **Configurazione > ASA Firepower Configuration > Object Management > PKI > Internal Certs** (Configurazione > ASA Firepower > Gestione oggetti > PKI > Certificati interni), quindi fare clic su **Add Internal Cert** (Aggiungi certificato interno).

Come illustrato nell'immagine, specificare il nome del certificato. Selezionare **Sfoglia** per selezionare il certificato dal computer locale oppure copiare e incollare il contenuto del certificato nei **dati** del **certificato**. Per specificare la chiave privata del certificato, sfogliare il file di chiave o copiare e incollare la chiave nell'opzione **Chiave**.

Se la chiave è crittografata, selezionare la casella di controllo **Encrypted** e specificare la password, come mostrato nell'immagine:

O O ASA FirePOWER Configurat	O O Configuration > ASA FirePOWER Configuration > Object Management > PKI > Internal Certs
Application Filters	
VRL	Add Internal Cort
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	nzANBakahkiG9w0BAQEFAAQBiQAwaYkCaYEA0uciKK9ofSyrAbYkSKC/nvy2a7Mi
🔻 🔦 РКІ	RHbV0ÜEK+2a5u5fDvZIRURHHBEbFp+SV0E7ak7PljdXd/sB4nhvvfPe4FN65IurN
🖶 Internal CAs	mjzYywUy4zi8u5z0r/9YhNJoz/2I2dvR4uZIPA9AQqXyveCCZ/OCQmFQ0rP6+qbk
🖶 Trusted CAs	Lrcyns+IrbHTJhge0Z2HC/XJmYwyJXhBuEavUgax-GhO99iNCOlo0iPIGFJnagBt
🖶 External Certs	Ftl7ohmI/F544x75fm17t3XwfZF/VA2GhG3W3QGFKHCA0U7CBaU78jCVBa9CTKOG
😝 Internal Certs	u8ceNhyAxU7MogAXN0ecqCW88w==
🐥 Internal CA Groups	
👫 Trusted CA Groups	
🔥 Internal Cert Group:	Key or, choose a file: Browse
🔒 External Cert Group	BEGIN RSA PRIVATE KEY
▶ 🏦 Local	MIICXAIBAAKBgQDSSyMor2h9LkSBtiRIoL+e/LaDsyNEdtXRQQr7Zrm7l809khFR
System Information	mip/Yi729Hi5nIB00BCne/HiTW81CV4K6yf6nUT418kt/3AXEGC6k0IDAOAB
dupdates	AoGBAJ+XOAu5cCAIhP6ujZZHzbjJEnNmQvGz2uiVh3HlsfY6SWxR87ic8zRROZBq
🛂 Licenses	cNNIWC4cm0BQ7cOwcZVzHi46ZZhEqrQOEeBr04B2BHwLZUFWergZnsna2sUbdsJ9
🔻 🚔 Tools	+filzEJWX4LgmXk8N887DkVC3fHVY5220fSVCal2C0AGbXN4BAKEA+fik0e10gX02 Pamzaf68lan4k/1WhaRib72DMV2PSVC7DNbhRfbv/thraG1ViG1Fr4bit2SFP5v
Backup Restore	d7QmDkGwyQJBANeOlVWWjBPuFCLQjYL04c66km9vzGgLDHjGc4gOING1iFlCrQt1
Cabaduling	
	Encrypted, and the password is:
A Device Setup	
	Store ASA FirePOWER Changes Cancel

Fare clic su Store ASA FirePOWER Changes per salvare il contenuto del certificato.

Passaggio 2. Importare il certificato CA (facoltativo).

Per i certificati server firmati da un certificato CA intermedio interno o radice, è necessario importare la catena interna di certificati CA nel modulo firepower. Al termine dell'importazione, il modulo firepower è in grado di convalidare il certificato del server.

Per importare il certificato CA, selezionare Configurazione > Configurazione ASA Firepower > Gestione oggetti > CA attendibili e fare clic su Aggiungi CA attendibile per aggiungere il certificato CA.

Passaggio 3. Configurare il criterio SSL.

Il criterio SSL definisce l'azione e i dettagli del server per cui si desidera configurare il metodo Decrypt-known per decrittografare il traffico in entrata. Se si dispone di più server interni, configurare più regole SSL in base a server diversi e al traffico che gestiscono.

Per configurare il criterio SSL, selezionare **Configura > Configurazione ASA FirePOWER > Criteri > SSL** e fare clic su **Aggiungi regola**.

Nome: specificare il nome della regola.

Azione: specificare l'azione come **Decrittografa - nota** e scegliere il certificato CA dall'elenco a discesa configurato nel passaggio precedente.

Definire la condizione in modo che corrisponda a queste regole, poiché sono disponibili più opzioni (rete, applicazione, porte e così via) specificate per definire il traffico interessante del server per il quale si desidera abilitare la decrittografia SSL. Specificare la CA interna nella scheda CA attendibili selezionate nella scheda Certificato CA attendibili.

Per generare gli eventi di decrittografia SSL, abilitare l'opzione di registrazione all'accesso.

○ ○ ○ ASA FirePOWER Configurat	○ ○ ○ Configuration >	ASA FirePOWER Co	nfiguration	> Policies :	> <u>SSL</u>					
Vertical Policies										
3 Access Control Policy	Default SSL Po	licy								
V S Intrusion Policy	SSL Policy									
Intrusion Policy	,									
🔊 Rule Editor										
Files				-						
Actions Alerts	Rules Trusted CA Cert	ificates Undecryp	table Actions	5						
Actions Alerts A Identity Policy	Add Bule									2 X
DNS Policy	Add Rule									
Device Management	Name Web Server Decr	vnt			Enabled	т	nsert below rule		¥ 1	
🔻 🧒 Object Management		, pr					below rule			
🕨 🔮 Network	Action 🔂 Decrypt - Know	wn Key 💙 wit	h web.serve	ertest.com		Edit				
▶ 🗩 Port	Zones Networks	Lisers Applicati	De Porte	Category	Certificate DN	Cert Status	Cipher Suite	Version		Logging
Security Zones		Applicati		cutegory	Continente Di		cipiter build	Verbion		Logging
Y Application Filters	Available Networks C				Source Networks	(0)		Destina	tion Networks (1)	
	Search by name or value	16			any			2 192	.168.10.5/32	<u> </u>
Variable Set	Networks	Geolocatio	·							
SecurityIntelligence	Private Networks	1								
Sinkhole				Add to						
FileList				Source						
🔅 Cipher Suite List				Add to						
Ø Distinguished Name										
🔻 🔍 РКІ										
🖶 Internal CAs										
Trusted CAs										
🐸 External Certs										
					Enter an IP addres	s	Add	Enter a	n IP address	Add
Device Setup										Add Cancel

Fare clic su Add per aggiungere la regola SSL.

E quindi fare clic su Store ASA Firepower Changes per salvare la configurazione del criterio SSL.

Passaggio 4. Configurare i criteri di controllo di accesso.

Dopo aver configurato il criterio SSL con le regole appropriate, è necessario specificare il criterio SSL nel controllo di accesso per implementare le modifiche.

Per configurare il criterio di controllo dell'accesso, selezionare **Configurazione > Configurazione di** ASA Firepower > Criteri > Controllo dell'accesso.

Fare clic sull'opzione **None** accanto a **SSL Policy** (Criterio SSL) oppure selezionare **Advanced** (Avanzate) > SSL Policy Setting (Impostazione criterio SSL), specificare il criterio SSL dall'elenco

a discesa e fare clic su OK per salvarlo.

Clic Archivia modifiche ASA Firepower per salvare la configurazione del criterio SSL.

Ènecessario distribuire i criteri di controllo di accesso. Prima di applicare il criterio, è possibile visualizzare un'indicazione relativa ai criteri di controllo di accesso non aggiornata nel modulo. Per distribuire le modifiche al sensore, fare clic su **Distribuisci** e scegliere l'**opzione Distribuisci modifiche FirePOWER. Verificare le modifiche apportate e fare clic su Distribuisci** nella finestra popup.

Nota: Nella versione 5.4.x, se è necessario applicare la policy di accesso al sensore, fare clic su **Apply ASA FirePOWER Changes** (Applica modifiche FirePOWER ASA).

Nota: Selezionare Monitoraggio > Monitoraggio di ASA Firepower > Stato task. È quindi necessario richiedere le modifiche alla configurazione per assicurarsi che l'attività sia stata completata.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

 Per la connessione SSL in uscita, dopo aver esplorato un sito Web SSL pubblico dalla rete interna, il sistema visualizza un messaggio di errore del certificato. Controllare il contenuto del certificato e verificare le informazioni sulla CA. Viene visualizzato il certificato CA interno configurato nel modulo Firepower. Accettare il messaggio di errore per sfogliare il certificato SSL. Per evitare la visualizzazione del messaggio di errore, aggiungere il certificato CA all'elenco delle CA attendibili del browser.

C Q Search

х

Certificate Viewer:"www.cisco.com"

<u>G</u>eneral <u>D</u>etails

Could not verify this cer	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

 Controllare gli eventi di connessione per verificare quali criteri SSL e la regola SSL sono interessati dal traffico. Selezionare Monitoraggio > ASA FirePOWER Monitoring > Real-Time Eventing. Selezionare un evento e fare clic su Visualizza dettagli. Verificare le statistiche di decrittografia SSL.

Filter Conr ASA f Reas Receiv 6/7/16	Inection Event Allo FirePOWER firewall connect son: Event Details Initiator Initiator IP	w	Besponder	Time: Wed 6/7/16 6:	29:10 AM (IST) to	Wed 6/7/16 6:29:11 AM (IST)
Re Receive 6/7/16	Event Details Initiator Initiator IP		Bornondor			
Receiv 6/7/16	Initiator Initiator IP		Pospondor			
6/7/16	Initiator IP		Responder		Traffic	
		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	incido
6/7/16	User	Special Identities/No Authentication Required	LIRI	http://www.aires.com	Egress Interface	outside
		Automoted	URL Catagony	nttps://cisco-tags.cisco.com /	TCP Flags	0
6/7/16	Transaction		URL Category	Pisk unknown	NetBIOS Domain	not available
6/7/16	Initiator Packets	4.0	HTTP Response	0		
0///10	Responder Packets	9.0	ППП Ксаронас	0	DNS	
6/7/16	Total Packets	13.0	Application		DNS Query	not available
0,7,20	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
C 17 11 C	Firewall Policy Rule/SI	Intrusion_detection	Client Tag	SSL protocol	SSL Rule	Outboound_SSL_Decrypt
6/7/16	Manitar Dulas	net suslishis	Web Application	Cisco	SSL Version	TLSv1.0
6/7/16	Monitor Kules	not 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	

- Verificare che la distribuzione dei criteri di controllo di accesso venga completata correttamente.
- Verificare che i criteri SSL siano inclusi nei criteri di controllo di accesso.
- Verificare che i criteri SSL contengano regole appropriate per la direzione in entrata e in uscita.
- Verificare che le regole SSL contengano la condizione corretta per definire il traffico di interesse.
- Monitorare gli eventi di connessione per verificare il criterio SSL e la regola SSL.
- Verificare lo stato di decrittografia SSL.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

Documentazione e supporto tecnico – Cisco Systems