Configure el descifrado SSL en el módulo FirePOWER mediante ASDM (administración integrada)

Contenido

Introducción **Prerequisites Requirements Componentes Utilizados Antecedentes** Descifrado SSL saliente Descifrado SSL entrante Configuración para el Descifrado SSL Descifrado SSL saliente (descifrado - renuncia) Paso 1. Configure el certificado de CA. Paso 2. Configure la política SSL. Paso 3. Configuración de la política de control de acceso Descifrado SSL entrante (descifrado - conocido) Paso 1. Importe el certificado y la clave del servidor. Paso 2. Importe el certificado de CA (opcional). Paso 3. Configure la política SSL. Paso 4. Configure la política de control de acceso. Verificación Troubleshoot Información Relacionada

Introducción

Este documento describe la configuración del descifrado de Secure Sockets Layer (SSL) en el módulo FirePOWER mediante ASDM (administración integrada).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento del firewall ASA (Adaptive Security Appliance), ASDM (Adaptive Security Device Manager)
- Conocimiento del appliance FirePOWER
- Conocimiento del protocolo HTTPS/SSL

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Módulos ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) que ejecutan la versión de software 6.0.0 y superiores
- Módulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) que ejecuta la versión de software 6.0.0 y posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Nota: Asegúrese de que FirePOWER Module tenga una licencia **Protect** para configurar esta funcionalidad. Para verificar la licencia, navegue hasta **Configuration > ASA FirePOWER Configuration > License**.

Antecedentes

Firepower Module descifra e inspecciona las conexiones SSL entrantes y salientes que se le redirigen. Una vez que se descifra el tráfico, se detectan y controlan las aplicaciones tunelizadas como el chat de facebook, etc. Los datos descifrados se inspeccionan en busca de amenazas, filtrado de URL, bloqueo de archivos o datos maliciosos.

Descifrado SSL saliente

El módulo firepower actúa como proxy de reenvío para las conexiones SSL salientes interceptando las solicitudes SSL salientes y regenerando un certificado para el sitio que el usuario desea visitar. La autoridad emisora (CA) es el certificado firmado automáticamente por Firepower. Si el certificado de firepower no forma parte de una jerarquía que existe o si no se agrega a la memoria caché del navegador de un cliente, el cliente recibe una advertencia mientras navega a un sitio seguro. El método Decrypt-Resignmethod se utiliza para realizar el descifrado SSL saliente.

Descifrado SSL entrante

En el caso del tráfico entrante a un servidor Web o dispositivo interno, el administrador importa una copia del certificado del servidor protegido y la clave. Cuando el certificado del servidor SSL se carga en el módulo firepower y la política de descifrado SSL se configura para el tráfico entrante, el dispositivo descifra e inspecciona el tráfico a medida que reenvía el tráfico. A continuación, el módulo detecta contenido malicioso, amenazas y malware que fluyen a través de este canal seguro. Además, el método de clave conocido por descifrado se utiliza para realizar el descifrado SSL entrante.

Configuración para el Descifrado SSL

Hay dos métodos de descifrado de tráfico SSL.

- Descifrar: renuncia para tráfico SSL saliente
- Descifrado: conocido para tráfico SSL entrante

Descifrado SSL saliente (descifrado - renuncia)

El módulo Firepower actúa como MITM (man-in-the-middle) para cualquier negociación SSL para servidores SSL públicos. Renuncia al certificado del servidor público con un certificado CA intermedio que se configura en el módulo firepower.

Estos son los tres pasos para configurar el Descifrado SSL saliente.

Paso 1. Configure el certificado de CA.

Configure un certificado autofirmado o un certificado CA de confianza intermedia para la renuncia del certificado.

Configuración del certificado de CA firmado automáticamente

Para configurar el certificado de CA firmado automáticamente, navegue hasta **Configuration > ASA Firepower Configuration > Object Management > PKI > Internal CAs** y haga clic en **Generate CA**. El sistema solicita los detalles del certificado de CA. Como se muestra en la imagen, complete los detalles según sus necesidades.

ASA FirePOWER Configur 🗗 🗜	Configuration > ASA FirePOWER Configurat	tion > Object Management > <u>PKI</u> > <u>Internal CAs</u>
ASA FirePOWER Configur D Network Network Network Network Network Network Network Security Zones Application Filters URL GeoLocation Variable Set SecurityIntelligence Sinkhole FileList Cipher Suite List Distinguished Name PKI Network Trusted CAs External Certs Internal CAS FineList Local Network Device Setup	Name Generate Internal Name: Country Name (two-least or Province: State or Province: Locality or City: Organizational Unit (East or Name) Common Name:	Certificate Authority ServerCA Internal CAs Internal CAs Certificate Authority ServerCA Internal CAs Internal Cas
Device Setup	Generate CSR	Generate self-signed CA Cancel
Remote Access VPN		No data to display 🛛 🌾 🦿 Pag
Site-to-Site VPN		
ASA FirePOWER Configuration		

Haga clic en **Generar CA autofirmada** para generar el certificado de CA interno. A continuación, haga clic en **Generar CSR** para generar la solicitud de firma de certificado que, en consecuencia,

se comparte con el servidor de la CA para firmar.

Configuración del certificado de CA intermedio

Para configurar el Certificado CA intermedio firmado por otra CA de terceros, navegue hasta Configuration > ASA Firepower Configuration > Object Management > PKI > Internal CAs y haga clic en Import CA.

Especifique el nombre del certificado. Seleccione **examinar** y cargar el certificado desde la máquina local o copie y pegue el contenido del certificado en la opción **Datos de certificado**. Para especificar la clave privada del certificado, navegue por el archivo de claves o copie y pegue la clave en la opción **Key**.

Si la clave está cifrada, active la casilla de verificación **Encrypted** y especifique la contraseña. Haga clic en **Aceptar** para guardar el contenido del certificado, como se muestra en la imagen:

Configuration > ASA FirePOWE	R Configuration > Object Management > PKI > Internal CAs	
ASA FirePOWER Configuration 🗉		
Network	Generate CA	Import CA
Application Filters	Import Internal Certificate Authority	? ×
	Name: Intermediate-CA	
	Certificate Data or, choose a file: Browse	
Ö Sinkhole ∑ FileList ≡ Cipher Suite List	CBMCS0ExEjAQBgNVBAcTCUJBTkdBTE9SRTEOMAwGA1UEChMFQ0ITQ08xDDAKBgNV BAsTA1RBQ2EaMBgGA1UEAxMRQ0Euc2VydmVydGVzdC5jb20xIzAhBgkqhkiG9w0B CQEWFGFkbWluQHNlcnZlcnRlc3QuY29tggkA9OflOUfXIF0wDAYDVR0TBAUwAwEB	•
Distinguished Name PKI More Internal CAs	/zANBgkqhkiG9w0BAQUFAAOBgQCXQME24zt0sKTzghQI5HuNWQl7NQlK3ZS5juVF YY24BJinUUiW5mCAID1K5yG+Jx26QlbWRs4vwfl8Fq3Dct0kRg74QpOzZS8l83F9 kuIpr+e7T+QifHbG4AzF5b2WGF4HUCxXjYTKtVHwbLuNeED5cAB38jL7Vso0cvg2 Biot1wc=	
😁 Trusted CAs	END CERTIFICATE	•
Internal Certs	Key or, choose a file: Browse	
Trusted CA Groups Trusted CA Groups Trusted Cert Groups Fyternal Cert Groups Trusted Cert Groups	i/DnuBs9S3UgPnN3xShcwMTg8N+1yWOTJnfIpar/0LpW4Eqn5izAEAcTzNmA4gR/ 3XMIL1RbCFUpUyL9D2N+4TuZzHrbmUa6QA1qPNwLcf0Vf1wgVyagZYYAn5oA50wA K554gAeIvYJC5dEXe9974K9nh7/hNG5B53S3gKuGGvQx+0DSilZy0J0RPzRnQmew cNshT03TGcdt6n58c1EcTWYZ3wavQCba1H02NcG0Ucfdl22/vsIavC0wn+61Kg72	•
A Device Setup	jIgYPD5KzjJ5AX9BRKFXbsSAFJ3bSZ9Ztx/jFlvaMdjEUqqctEP69Fav6sQdTDo wFkMModFPeSBol7WLTjKujyRLM0/p7bsM41Wdn4x1J2j2k+E9AWoXw+kGF9PwNBQ	
Firewall	END RSA PRIVATE KEY	L
Remote Access VPN	Encrypted, and the password is:	
Site-to-Site VPN		
ASA FirePOWER Configuration	ОК	Cancel

Paso 2. Configure la política SSL.

La política SSL define la acción de descifrado e identifica el tráfico en el que se aplica el método de descifrado de renuncia. Configure las distintas reglas SSL en función de los requisitos empresariales y la política de seguridad de la organización.

Para configurar la política SSL, navegue hasta **Configurar > ASA FirePOWER Configuration > Políticas > SSL** y haga clic en **Agregar regla**.

Nombre: Especifique el nombre de la regla.

Acción: Especifique la acción como Descifrar - Renunciar y elija el certificado de CA de la lista

desplegable que se configuró en el paso anterior.

Defina las condiciones en la regla para que coincidan con el tráfico, ya que hay varias opciones (zona, red, usuarios, etc.), especificadas para definir el tráfico que se debe descifrar.

Para generar los eventos de descifrado SSL, habilite la opción **registro** de registro, como se muestra en la imagen:

O O ASA FirePOWER Configurat	O O Configuration > ASA Fire	POWER Configuration > Polic	ies > SSL		
▼ <i>I</i> Policies					
🚦 Access Control Policy	Default SSL Policy				
Intrusion Policy	SSL Policy				
Files	,				
SSL					
Actions Alerts					
	Rules Trusted CA Certificates	Undecryptable Actions			
Division Management				Add Category Add R	ile Search Rules 💥
Object Management					
► 🏠 Local	Add Rule				? ×
System Information					
📑 Updates	Name Outboound_SSL_Decrypt		C Enabled	Insert into Category	▼ Standard Rules
🏭 Licenses	Action G Decrypt - Resign	✓ with ServerCA	× .	🖒 🗌 Replace Key	
Tools		· · · ·			
🕨 🔌 Integration	Zones Networks Users	Applications Ports Cate	gory Certificate DN Cert S	Status Cipher Suite Version	Logging
	Available Networks 🖒	•	Source Networks (1)	Destination	Networks (0)
	Search by name or value		🚍 Private Networks	any any	
	Naturata	Contention			
	Networks	Geolocation			
	Private Networks				
		Sour	ce		
		Add	to		
		Destina	ation		
💑 <u>D</u> evice Setup			Enter an IP address	Add Enter an IF	address Add
Firewall					Add Cancel
Remote Access VPN					
Site-to-Site VPN				No. 4-	ra ta diaplay 1/ / Daga 1af 1
ASA FirePOWER Configur				NO da	a to display R Page 1 Of 1 2 2 C

Haga clic en Agregar para agregar la regla SSL.

Haga clic en Store ASA Firepower Changes para guardar la configuración de la política SSL.

Paso 3. Configuración de la política de control de acceso

Una vez que configure la política SSL con las reglas adecuadas, debe especificar la política SSL en el Control de acceso para implementar los cambios.

Para configurar la política de control de acceso, navegue hasta **Configuration > ASA Firepower Configuration > Policies > Access Control.**

Haga clic en **Ninguno** de la **política SSL** o navegue hasta **Avanzado > Configuración de la política SSL**. Especifique la política SSL en la lista desplegable y haga clic en **Aceptar** para guardarla, como se muestra en la imagen:

O O ASA FirePOWER Configurat	Configuration > ASA FirePOWER Configuration > Policies > Access (<u>Control I</u>
V Dolicies		
📳 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		
Gold Contract Management		
Local	Identity Policy: None SSL Policy: None	
Updates	Rules Security Intelligence HTTP Responses Advanced	
🔛 Licenses	General Settings	li)
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 ? X	Yes
	connections	Yes
		105
	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

Haga clic Almacenar cambios en el firewall ASA para guardar la configuración de la política SSL.

Debe implementar la política de control de acceso en el sensor. Antes de aplicar la política, hay una indicación de que la **Política de control de acceso está desactualizada** en el módulo. Para implementar los cambios en el sensor, haga clic en **Implementar** y seleccione la **opción Implementar cambios de FirePOWER.** Verifique los cambios realizados y haga clic en **Implementar.**

Nota: En la versión 5.4.x, si necesita aplicar la política de acceso al sensor, haga clic en **Aplicar cambios de FirePOWER ASA.**

Nota: Vaya a **Monitoring > ASA Firepower Monitoring > Task Status**. A continuación, se aplican los cambios de configuración para asegurarse de que la tarea se ha completado.

Descifrado SSL entrante (descifrado - conocido)

El método de descifrado SSL entrante (conocido por descifrado) se utiliza para descifrar el tráfico SSL entrante para el que ha configurado el certificado de servidor y la clave privada. Debe importar el certificado de servidor y la clave privada al módulo Firepower. Cuando el tráfico SSL llega al módulo Firepower, descifra el tráfico y realiza la inspección en el tráfico descifrado. Después de la inspección, el módulo Firepower vuelve a cifrar el tráfico y lo envía al servidor. Estos son los cuatro pasos para configurar el Descifrado SSL saliente:

Paso 1. Importe el certificado y la clave del servidor.

Para importar el certificado y la clave del servidor, navegue hasta **Configuration > ASA Firepower Configuration > Object Management > PKI > Internal Certs** y haga clic en **Add Internal Cert**.

Como se muestra en la imagen, especifique el nombre del certificado. Seleccione **examinar** para seleccionar el certificado de la máquina local o copiar y pegar el contenido del certificado en los **datos del certificado**. Para especificar la clave privada del certificado, navegue por el archivo de clave o copie y pegue la clave en la **clave** de opción.

Si la clave está cifrada, active la casilla de verificación **Encrypted** y especifique la contraseña, como se muestra en la imagen:

○ ○ ○ ASA FirePOWER Configurat ○ ○ ○	Configuration > ASA FirePOWER Configuration > Object Management > PKI > Internal	Certs
Application Filters		
► www URL	Add Internal Cort	Eil
😡 GeoLocation		
🔦 Variable Set 🛛 🛛 🙀	Add Known Internal Certificate	? X
SecurityIntelligence		
Sinkhole	Name: web.servertest.com	
📝 FileList		
🌼 Cipher Suite List	Certificate Data or, choose a file: Browse	
🕨 🗐 Distinguished Name	nzANBgkghkiG9w0BAQEFAAOBjQAwgYkCgYEA0ucjKK9ofSyrAbYkSKC/nvy2g7Mj	
🔻 🔦 РКІ	RHbV0UEK+2a5u5fDvZIRURHHBEbFp+SV0E7ak7PljdXd/sB4nhvvfPe4FN65IurN	
😆 Internal CAs	mjzYywUy4zi8uSzOr/9YhNJoz/212dvR4uZ1PA9AQqXvyeCCL/OCQmFQOrP6+qbk +FPHI f9wFyRahaFCAwFAATANRakahkiG9w0BAOsFAAORaOCuk7VPuTai]euiPrF	
😝 Trusted CAs	Lrcyns+lrbHTJhge0Z2HC/XJmYwyJXhBuEqvU9qx+GhQ99jNCOlo0iPIGF1naqBt	
😝 External Certs	FtI7ohmI/F544x75fm17t3XwfZF/VA2GhG3W3QGFKHCA0U7CBaU78jCVBa9CTKOG	
😁 Internal Certs	uscennyaxu/mogaxnuecqc.wssw==	
👶 Internal CA Groups		
👶 Trusted CA Groups		
👶 Internal Cert Group:	Key or, choose a file: Browse	
👶 External Cert Group	BEGIN RSA PRIVATE KEY	
🕨 🏠 Local	MILCXALBAAKBGQUSSyMor2h9LKsBtiRIoL+e/LaDsyNEdtXRQQr/2rm/I809khFR EccERsWn51XOTtoTs+WN1d3+wHieG+9897aLl3rki6s2aPNiLBTLiOLy5LM6y/1iE	
🔄 System Information	0mjP/YjZ29Hi5nU8D0BCpe/J4IIv84JCYVA6s/r6puT4U8ct/3AXEGCGkQIDAQAB	
📑 Updates	AoGBAJ+XOAu5cCAIhP6ujZZHzbjJEnNmQvGz2uiVh3HlsfY6SWxR87ic8zRROZBq	
🔡 Licenses	+nzEJwx4LamXR8N88YbkyC3n4iVY5z90fsvCdJ2UoAGBXN4BAkEA+nkDe1UalxOz	
🔻 💼 Tools	Pgmzad68lngk4/7Wbg8ibZz0Mv2PSvO7pNbhRfpy/dtgGLJvIGJIr/+0iL2SrPFv	
🗑 Backup Restore	d7QmDkGwyQJBANeOlVWWjBPuFCLQjYL04c66km9vzGgLDHjGc4gOING1iFlCrQt1	
Cahadulina	Encrypted, and the password is:	
💑 <u>D</u> evice Setup	Store ASA FireDOWED Changes	

Haga clic en Store ASA FirePOWER Changes para guardar el contenido del certificado.

Paso 2. Importe el certificado de CA (opcional).

Para el certificado de servidor firmado por el certificado de CA interna intermedia o raíz, debe importar la cadena interna de certificados de CA al módulo de firepower. Una vez realizada la importación, el módulo firepower puede validar el certificado del servidor.

Para importar el certificado de CA, navegue hasta **Configuration > ASA Firepower Configuration > Object Management > Trusted CAs** y haga clic en **Add Trusted CA** para agregar el certificado de CA.

Paso 3. Configure la política SSL.

La política SSL define la acción y los detalles del servidor para los cuales desea configurar el método conocido de descifrado para descifrar el tráfico entrante. Si tiene varios servidores internos, configure varias reglas SSL basadas en diferentes servidores y el tráfico que manejan.

Para configurar la política SSL, navegue hasta **Configurar > Configuración de ASA FirePOWER > Políticas > SSL** y haga clic en **Agregar regla**.

Nombre: Especifique el nombre de la regla.

Acción: Especifique la acción como **Descifrar - conocido** y elija el certificado CA de la lista desplegable que se configura en el paso anterior.

Defina la condición para que coincida con estas reglas, ya que hay varias opciones (red, aplicación, puertos, etc.) especificadas para definir el tráfico interesante del servidor para el que desea habilitar el descifrado SSL. Especifique la CA interna en las **CAs de confianza** seleccionadas en la ficha de certificado de CA de confianza.

Para generar los eventos de descifrado SSL, habilite la opción logging logingat.

○ ○ ○ ASA FirePOWER Configurat	○ ○ ○ <u>Configuration > </u>	ASA FirePOWER Config	uration > Policies	> <u>SSL</u>			
V Dolicies							
3 Access Control Policy	Default SSL Pol	icv					
Intrusion Policy		,					
Intrusion Policy	SSL Policy						
👼 Rule Editor							
🖺 Files							
🔒 SSL	Rules Trusted CA Cert	ificates Undecryptable	e Actions				
🔯 Actions Alerts							
ldentity Policy	Add Rule						? ×
DNS Policy							
Device Management	Name Web_Server_Decry	/pt		Enabled	Insert below rule	✓ 1	
🔻 🧑 Object Management	Action 🗿 Decrupt - Know	with	web convertent com		Edit		
Network	Action Decrypt - Know	in Key	web.servertest.com		Lucit		
Port	Zones Networks	Users Applications	Ports Category	Certificate DN	Cert Status Cipher Suite	Version	Logging
Security Zones			() () () () () () () () () () () () () (Course Numeral of (C		Desting the Networks (1)	
Y Application Filters				Source Networks (U	((Destination Networks (1)	
	Search by name or valu	e		any		192.168.10.5/32	
GeoLocation	Networks	Geolocation					
Security Intelligence	Private Networks	1					
Sinkhole			Add to				
Filel ist			Source				
Cinher Suite List			Add to				
Distinguished Name							
V Q PKI							
🖶 Internal CAs							
🖶 Trusted CAs							
🖶 External Certs							
				Enter an IP address	Add	Enter an IP address	Add
S Device Setup							
							Add Cancel

Haga clic en Agregar para agregar la regla SSL.

Y luego haga clic en **Store ASA Firepower Changes** para guardar la configuración de la política SSL.

Paso 4. Configure la política de control de acceso.

Una vez que configure la política SSL con las reglas adecuadas, debe especificar la política SSL en el Control de acceso para implementar los cambios.

Para configurar la política de control de acceso, navegue hasta **Configuration > ASA Firepower Configuration > Policies > Access Control.**

Haga clic en la opción **None** junto a **SSL Policy** o navegue hasta **Advanced > SSL Policy Setting**, especifique la política SSL en la lista desplegable y haga clic en **OK** para guardarla.

Haga clic Almacenar cambios en el firewall ASA para guardar la configuración de la política SSL.

Debe implementar la política de control de acceso. Antes de aplicar la política, puede ver una indicación de Directiva de control de acceso desactualizada en el módulo. Para implementar los cambios en el sensor, haga clic en **Implementar** y elija la **opción Implementar cambios de FirePOWER.** Verifique los cambios realizados y haga clic en **Implementar** en la ventana emergente.

Nota: En la versión 5.4.x, si necesita aplicar la política de acceso al sensor, haga clic en **Aplicar cambios de ASA FirePOWER**.

Nota: Vaya a **Monitoring > ASA Firepower Monitoring > Task Status**. A continuación, se aplican los cambios de configuración para asegurarse de que la tarea se ha completado.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

 Para la conexión SSL saliente, una vez que navega por un sitio web público de SSL desde la red interna, el sistema envía un mensaje de error del certificado. Verifique el contenido del certificado y verifique la información de CA. Aparece el certificado de CA interno que configuró en el módulo Firepower. Acepte el mensaje de error para examinar el certificado SSL. Para evitar el mensaje de error, agregue el certificado de CA a la lista de CA de confianza de su navegador.

C Q Search

х

Certificate Viewer: "www.cisco.com"

General Details

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:
en kana en uwa kakamananan kara 📼 man 2001 kanakan ka	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

 Verifique los eventos de conexión para verificar qué política SSL y regla SSL están en el tráfico. Vaya a Monitoring > ASA FirePOWER Monitoring > Real-Time Event.Seleccione un evento y haga clic en Ver detalles. Verifique las estadísticas de descifrado SSL.

All ASA	A FirePOWER Events Connecti	on Intrusion File Malwa	re File Security Intelligence			
ilter	Connection Event Allo ASA FirePOWER firewall connect	w tion event		Time: Wed 6/7/16 6:	: 29:10 AM (IST) to	Wed 6/7/16 6:29:11 AM (IST)
	Reason:					
🕨 Re	Event Details					
Receive	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	ingido
6/7/16	User	Special Identities/No Authentication Required	LIRI	https://sizes.tess.sizes.com/	Egress Interface	outside
		Addictideation Required	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	ПППКсэропэс	0	DNS	
6/7/16	Total Packets	13.0	Application		DNS Query	not available
0,7,120	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/7/1C	Firewall Policy Rule/SI	Intrusion_detection	Client Tag	SSL protocol	SSL Rule	Outboound_SSL_Decrypt
6/7/16	Manitar Bulas	not susilabla	Web Application	Cisco	SSL Version	TLSv1.0
6/7/16	Monitor Rules	not avallable	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

- Asegúrese de que la implementación de la política de control de acceso se complete correctamente.
- Asegúrese de que la política SSL está incluida en la política de control de acceso.
- Asegúrese de que la política SSL contiene las reglas adecuadas para la dirección entrante y saliente.
- Asegúrese de que las reglas SSL contengan la condición adecuada para definir el tráfico interesante.
- Supervise los eventos de conexión para verificar la política SSL y la regla SSL.
- Verifique el estado de descifrado SSL.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

Soporte Técnico y Documentación - Cisco Systems