Configure a descriptografia SSL no módulo FirePOWER usando ASDM (On-Box Management, gerenciamento integrado)

Contents

Introduction **Prerequisites Requirements Componentes Utilizados** Informações de Apoio Descriptografia SSL de saída Descriptografia SSL de entrada Configuração para descriptografia de SSL Descriptografia SSL de saída (Descriptografia - Reassinatura) Etapa 1. Configure o certificado CA. Etapa 2. Configure a política SSL. Etapa 3. Configurar a política de controle de acesso Descriptografia SSL de entrada (descriptografar - conhecido) Etapa 1. Importar o certificado e a chave do servidor. Etapa 2. Importar o certificado CA (opcional). Etapa 3. Configure a política SSL. Etapa 4. Configure a política de controle de acesso. Verificar Troubleshoot Informações Relacionadas

Introduction

Este documento descreve a configuração da descriptografia SSL (Secure Sockets Layer) no módulo FirePOWER usando ASDM (On-Box Management, gerenciamento integrado).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do firewall ASA (Adaptive Security Appliance), ASDM (Adaptive Security Device Manager)
- Conhecimento do dispositivo FirePOWER
- Conhecimento do protocolo HTTPS/SSL

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Módulos ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) executando a versão de software 6.0.0 e superior
- Módulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X) executando a versão de software 6.0.0 e superior

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.

Note: Verifique se o FirePOWER Module tem uma licença **Protect** para configurar essa funcionalidade. Para verificar a licença, navegue para **Configuration > ASA FirePOWER Configuration > License**.

Informações de Apoio

O módulo Firepower descriptografa e inspeciona as conexões SSL de entrada e saída que são redirecionadas para ele. Depois que o tráfego é descriptografado, aplicativos em túnel, como bate-papo no facebook etc., são detectados e controlados. Os dados descriptografados são inspecionados para verificar se há ameaças, filtragem de URL, bloqueio de arquivos ou dados mal-intencionados.

Descriptografia SSL de saída

O módulo firepower atua como o proxy de encaminhamento para conexões SSL de saída interceptando solicitações SSL de saída e regerando um certificado para o site que o usuário deseja visitar. A autoridade emissora (AC) é o certificado com assinatura automática do Firepower. Se o certificado do firepower não fizer parte de uma hierarquia existente ou se não for adicionado ao cache do navegador de um cliente, o cliente receberá um aviso enquanto navega para um site seguro. O método Decrypt-Resignmethod é usado para executar a descriptografia de SSL de saída.

Descriptografia SSL de entrada

No caso de tráfego de entrada para um servidor Web interno ou dispositivo, o administrador importa uma cópia do certificado do servidor protegido e a chave. Quando o certificado do servidor SSL é carregado no módulo firepower e a política de descriptografia SSL é configurada para o tráfego de entrada, o dispositivo então descriptografa e inspeciona o tráfego à medida que ele encaminha o tráfego. O módulo, então, detecta conteúdo mal-intencionado, ameaças e malware fluindo por esse canal seguro. Além disso, o método Disrypt-Known Keymethod é usado para executar a descriptografia SSL de entrada.

Configuração para descriptografia de SSL

Há dois métodos de descriptografia de tráfego SSL.

- Descriptografar Reiniciar para tráfego SSL de saída
- Descriptografar conhecido para tráfego SSL de entrada

Descriptografia SSL de saída (Descriptografia - Reassinatura)

O módulo Firepower atua como MITM (man-in-the-middle) em qualquer negociação SSL para servidores SSL públicos. Ele rende o certificado do servidor público por um certificado CA intermediário que está configurado no módulo firepower.

Estas são as três etapas para configurar a Descriptografia SSL de saída.

Etapa 1. Configure o certificado CA.

Configure um certificado autoassinado ou um certificado CA confiável intermediário para a renúncia do certificado.

Configurar o certificado CA com assinatura automática

Para configurar o certificado CA com assinatura automática, navegue para **Configuration > ASA Firepower Configuration > Object Management > PKI > Internal CAs** e clique em **Generate CA**. O sistema solicita os detalhes do certificado CA. Como mostrado na imagem, preencha os detalhes conforme o seu requisito.

ASA FirePOWER Configur 리 무	Configuration > ASA FirePOWER Configuration > Object Management >	• <u>PKI</u> > <u>Internal CAs</u>
ASA FirePOWER Configur 2 7 Network Port Security Zones Application Filters URL GeoLocation Variable Set SecurityIntelligence Sinkhole FileList Cipher Suite List Distinguished Name	Name Generate Internal Certificate Authority Name: ServerCA Country Name (two-letter code): IN State or Province: KA	• <u>PKI</u> > <u>Internal CAs</u> ③ Generate CA ③ Import CA ? ×
PKI Trusted CAs External Certs Internal Certs Internal CA Groups Trusted CA Groups Internal Cert Groups Local	Locality or City: Bangalore Organization: TAC Organizational Unit (Department): TAC Common Name: serverCA.exa	ample.com
Device Setup Firewall Remote Access VPN Site-to-Site VPN ASA FirePOWER Configuration	Generate CSR	enerate self-signed CA Cancel No data to display <

Clique em **Gerar CA autoassinado** para gerar o certificado CA interno. Em seguida, clique em **Gerar CSR** para gerar a solicitação de assinatura de certificado que é compartilhada com o

servidor CA para assinar.

Configurar o certificado CA intermediário

Para configurar o Certificado CA intermediário assinado por outra CA de terceiros, navegue para Configuração > Configuração do ASA Firepower > Gerenciamento de objetos > PKI > CAs internas e clique em Importar CA.

Especifique o nome do certificado. Selecione **Procurar** e carregar o certificado da máquina local ou copie-cole o conteúdo do certificado na opção **Dados do certificado**. Para especificar a chave privada do certificado, navegue no arquivo de chave ou copie-cole a chave na opção **Key**.

Se a chave estiver criptografada, ative a caixa de seleção **Criptografada** e especifique a senha. Clique em **OK** para salvar o conteúdo do certificado, como mostrado na imagem:

Configuration > ASA FirePOWE	R Configuration > Object Management > PKI > Internal CAs	
ASA FirePOWER Configuration		
		-
Hetwork	Generate CA	mport CA
Port Security Zones	Import Internal Certificate Authority	? X
Application Filters		
URL	Name: Intermediate-CA	
GeoLocation		
Variable Set	Certificate Data or, choose a file: Browse	
Sickhole		
	RASTA1RROZEAMRAGA1LEAVMROOEuc2VvdmVvdGVzdC5ib20vIzAbRakabkiG9w0B	-
Cinber Suite List	COEWFGFkbWluOHNlcnZlcnRlc3OuY29taakA9OflOUfXIF0wDAYDVR0TBAUwAwEB	
Gipher Bare Eber	/zÄNBgkqhkiG9w0BAQUFAAOBgQCXQME24zt0sKTzghQI5HuNWQl7NQlK3ZS5juVF	
	YY24BJinUUiW5mCAlD1KSyG+Jx26QlbWRs4vwfl8Fq3Dct0kRg74QpOzZS8l83F9	
Internal CAs	kuIpr+e7T+QitHbG4AzF5b2WGF4HUCxXjYTKtVHwbLuNeED5cAB38jL7Vso0cvg2	
	BIALIW ==	
😝 External Certs		*
😁 Internal Certs		
	Key or, choose a file: Browse	
	i/Dou/Bo0C2UeBoN/2vChow/MTeRN + 1vM/OT1offact/01 pM/4EapEicAEAcTzNmA4eB/	
	3XMTI 1RbCFUpUvi 9D2N+4TuZzHrbmUa6OA1gPNwl cf0Vf1wgVvagZYYAn5oA50wA	22
Evternal Cert Groups	K554gAeIvYJC5dEXe9974K9nh7/hNG5B53S3gKuGGvQx+0DSilZy0J0RPzRnQmew	
	cNsbTQ3TGcdt6p58cJFsTWYZayvvQCbeJHOgNcGOUcfdlZ2/v6IoVC0wp+61KgZ7	
🔏 Device Setup	jIgYPD5KzjJ5AX9BRKFXbsSAFJ3bSZ9Ztx/jFlvaMdjEUqqctEPP69Fav6zSdTDo	
<u> </u>	WFKMM00FP65B0F/WEFJKUJYKLM0/p/D5M41W0N4X1J2J2K+E9AW0XW+K6F9PWNBQ 22WVRp02LliZWTKvSdLl0Mr4mDRVRkzb+Tab20D7/SZENWEpuktyW00A==	
🚰 Firewall	END RSA PRIVATE KEY	
Remote Access VPN	Encrypted and the password is:	×
Site-to-Site VPN		
ASA FirePOWER Configuration	OK Car	ncel

Etapa 2. Configure a política SSL.

A política SSL define a ação de descriptografia e identifica o tráfego no qual o método de descriptografia é aplicado. Configure as várias regras SSL com base nos requisitos de negócios e na política de segurança da empresa.

Para configurar a política SSL, navegue para **Configurar > Configuração do ASA FirePOWER > Políticas > SSL** e clique em **Adicionar regra**.

Nome: especifique o nome da regra.

Ação: Especifique a ação como **Descriptografar - Resign** e escolha o certificado CA na lista suspensa configurada na etapa anterior.

Defina as condições na regra para corresponder o tráfego, pois há várias opções (zona, rede, usuários, etc.), especificadas para definir o tráfego que precisa ser descriptografado.

Para gerar os eventos de descriptografia SSL, ative a opção de **registro** de log, como mostrado na imagem:

O O ASA FirePOWER Configurat	○ ○ ○ Configuration >	ASA FirePOWER	R Configuratio	on > Policies >	SSL					
Vertical Policies										
🐮 Access Control Policy	Default SSL Po	licy								
Intrusion Policy	SSL Policy	,								
Files	,									
E SSL										14 III
Actions Alerts		r								
Identity Policy DNS Reliev	Rules Trusted CA Cer	ificates Under	cryptable Actio	ns						<u> </u>
Device Management							Add Categor	y 💿 Add Rule	Search Rules	×
Object Management										
► 🏠 Local	Add Rule									? ×
System Information										
🚽 Updates	Name Outboound_SSL	Decrypt			Enabled	I	nsert into Categor	/	 Standard Rules 	~
🔢 Licenses	Action 🔂 Decrypt - Re	sign 🔽	with Server	CA		- c - i	Replace Key			
Tools		· · · ·					·			
🕨 🔌 Integration	Zones Networks	Users App	lications Por	ts Category	Certificate DN	Cert Status	Cipher Suite	Version		Logging
	Available Networks		œ		Source Networks	(1)		Destination Ne	tworks (0)	
	Search by name or va	lue			📻 Private Networ	ks	8	any		
	Networks	Geolo	cation							
	Private Networks		I							
				Add to						
				Source						
				Add to						
				Destination						
<u>Device Setup</u>					Enter an IP addres	S	Add	Enter an IP add	ress	Add
🕵 F <u>i</u> rewall									Add	Cancel
Remote Access VPN										
Site-to-Site VPN										
ASA FirePOWER Configur								No data to	display IC C Pagé 1	OLT > > C

Clique em Adicionar para adicionar a regra SSL.

Clique em Store ASA Firepower Changes para salvar a configuração da política SSL.

Etapa 3. Configurar a política de controle de acesso

Depois de configurar a política SSL com regras apropriadas, você deve especificar a política SSL no Controle de Acesso para implementar as alterações.

Para configurar a política de controle de acesso, navegue para **Configuration > ASA Firepower Configuration > Policies > Access Control.**

Clique em **None** of the **SSL Policy** ou navegue para **Advanced > SSL Policy Setting.** Especifique a política SSL na lista suspensa e clique em **OK** para salvá-la, como mostrado na imagem:

O O ASA FirePOWER Configurat	O O O Configuration > ASA FirePOWER Configuration > Policies > Access (<u>Control I</u>
▼ 🗐 Policies		
Access Control Policy	ASA ASA FirePOWER	
 Intrusion Policy Files SSL Actions Alerts Identity Policy DNS Policy DNS Policy Device Management Object Management Local 	Default Allow All Traffic Enter a description	
🔄 System Information		
📑 Updates	Rules Security Intelligence HTTP Responses Advanced	
Licenses	General Settings	Ø
Integration	Maximum IIRI characters to store in connection events	1024
megration		1024
	Allow an Interactive Block to bypass blocking for (seconds)	600
	Retry U SSL Policy to use for inspecting encrypted ? ×	Yes
	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

Clique em Armazene as alterações do ASA Firepower para salvar a configuração da política SSL.

Você deve implantar a política de controle de acesso no sensor. Antes de aplicar a política, há uma indicação de que a **Política de controle de acesso está desatualizada** no módulo. Para implantar as alterações no sensor, clique em **Implantar** e selecione a **opção Implantar alterações do FirePOWER.** Verifique as alterações feitas e clique em **Implantar**.

Note: Na versão 5.4.x, se precisar aplicar a política de acesso ao sensor, clique em Aplicar alterações do ASA FirePOWER.

Note: Navegue até **Monitoring > ASA Firepower Monitoring > Task Status.** Em seguida, você se inscreve para alterações de configuração para garantir que a tarefa seja concluída.

Descriptografia SSL de entrada (descriptografar - conhecido)

O método Descriptografia SSL de entrada (Descriptografia conhecida) é usado para descriptografar o tráfego SSL de entrada para o qual você configurou o certificado do servidor e a chave privada. Você precisa importar o certificado do servidor e a chave privada para o módulo Firepower. Quando o tráfego SSL atinge o módulo Firepower, ele descriptografa o tráfego e realiza a inspeção no tráfego descriptografado. Após a inspeção, o módulo Firepower criptografa novamente o tráfego e o envia ao servidor.

Estas são as quatro etapas para configurar a Descriptografia SSL de saída:

Etapa 1. Importar o certificado e a chave do servidor.

Para importar o Server Certificate and Key (Certificado e chave do servidor), navegue para Configuration > ASA Firepower Configuration > Object Management > PKI > Internal Certs (Configuração > Configuração do ASA Firepower > Gerenciamento de objetos > PKI > Certs internos) e clique em Add Internal Cert (Adicionar certificado interno).

Como mostrado na imagem, especifique o nome do certificado. Selecione **Procurar** para selecionar o certificado da máquina local ou copie-cole o conteúdo do certificado nos **Dados do certificado**. Para especificar a chave privada do certificado, navegue no arquivo de chave ou copie-cole a chave na opção **Key**.

Se a chave estiver criptografada, ative a caixa de seleção **Criptografada** e especifique a senha, como mostrado na imagem:

O O ASA FirePOWER Configurat	Configuration > ASA FirePOWER Configuration > Object Management > PKI > Internal Certs
Application Filters	
► WWW URL	Add Internal Cart
😡 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	mjzyywUy4zi8uSzOr/9YNNJoz/212dvR4u21PA9AQqXvyeCCL/UCQmFQOrP6+qbR +FPHI f9wFxBabpFCAwFAATANBakabkiG9w0BAOsFAAOBaOCukZVPuTai1euiPrtF
🖶 Trusted CAs	Lrcyns+lrbHTJhge0Z2HC/XJmYwyJXhBuEqvU9qx+GhQ99jNCOlo0iPIGF1naqBt
🖶 External Certs	FtI7ohmI/F544x75fm17t3XwfZF/VA2GhG3W3QGFKHCA0U7CBaU78jCVBa9CTKOG
🖶 Internal Certs	END CERTIFICATE
🐥 Internal CA Groups	
🐥 Trusted CA Groups	Key or choose a file:
🔒 Internal Cert Group:	
🚜 External Cert Group	BEGIN RSA PRIVATE KEY MIICYAIRAAKBAODSS:/Mar2bal.KeBtiDial.+a/l.aDc:/A/EdtYDOOr77rm7/800kbED
Local	EccERsWn5JXQTtgTs+WN1d3+wHieG+9897qU3rki6s2aPNjLBTLjOLy5LM6v/1iE
🔄 System Information	0mjP/YjZ29Hi5nU8D0BCpe/J4IIv84JCYVA6s/r6puT4U8ct/3AXEGCGkQIDAQAB
🛒 Updates	A0GBAJ+X0Au5cCAInP6uj2ZHzbjJEnNmQvGz2uiVh3HistY65WxR87iC8zRR02Bq cNNTWC4cm0R07cOwc7VzHi4677hEar00EeBr04B2BHwl ZI jEWera7ospa2si Jbds19
🟭 Licenses	+nzEJwx4LgmXR8N88YbkvC3n4iVY5z90fsvCdJ2UoAGBXN4BAkEA+nkDe1UglxOz
Tools	Pgmzad68lngk4/7Wbg8ibZz0Mv2PSvO7pNbhRfpy/dtgGLJvIGJIr/+0iL2SrPFv
🐼 Backup Restore	avównkowyójekikeolkwwjekałcróji rołcoekważcegropijecłegotke telefoti
Cabadulina	Encrypted, and the password is:
Device Setup	Store ASA FirePOWER Changes Cancel

Clique em Store ASA FirePOWER Changes para salvar o conteúdo do certificado.

Etapa 2. Importar o certificado CA (opcional).

Para o certificado do servidor assinado pelo certificado CA interno intermediário ou raiz, é necessário importar a cadeia interna de certificados CA para o módulo firepower. Após a importação ser realizada, o módulo firepower pode validar o certificado do servidor.

Para importar o certificado CA, navegue para **Configuration > ASA Firepower Configuration > Object Management > Trusted CAs** e clique em **Add Trusted CA** para adicionar o certificado CA. A política SSL define a ação e os detalhes do servidor para os quais você deseja configurar o método Descriptografar conhecido para descriptografar o tráfego de entrada. Se você tiver vários servidores internos, configure várias regras SSL com base em diferentes servidores e no tráfego que eles manipulam.

Para configurar a política SSL, navegue para **Configurar > Configuração do ASA FirePOWER > Políticas > SSL** e clique em **Adicionar regra**.

Nome: especifique o nome da regra.

Ação: Especifique a ação como **Descriptografar - conhecido** e escolha o certificado CA na lista suspensa configurada na etapa anterior.

Defina a condição para corresponder a essas regras, pois há várias opções (rede, aplicação, portas etc.) especificadas para definir o tráfego interessante do servidor para o qual você deseja habilitar a descriptografia SSL. Especifique a AC interna em **CAs confiáveis selecionadas na** guia **de certificado CA confiável.**

Para gerar os eventos de descriptografia de SSL, ative a opção de registro de log de log.

○ ○ ○ ASA FirePOWER Configurat	○ ○ ○ ○ Configuration	> ASA Fire	POWER Config	uration	> Policies >	- <u>SSL</u>								
V Dolicies														
Access Control Policy	Default SSL P	olicy												
Ontrusion Policy	SSL Policy													
Intrusion Policy Rule Editor														
Files														V 1
	Bules Trusted CA C	artificatos	Undecryptabl	o Actions	٦									
X Actions Alerts	Rules Husted CA C	ertificates	ondecryptabl	e Actions										
🚨 Identity Policy	Add Rule													? ×
DNS Policy														
Device Management	Name Web_Server_De	crypt				🔽 Enable	d	I	nsert I	elow rule		*	1	
Viet Wanagement	Action Action Action	iown Kev	✓ with	web.serve	rtest.com			Edit						
Network E Port			L									_		
Security Zones	Zones Network	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Ciph	er Suite	Version			Logging
Application Filters	Available Networks	;		•		Source Netw	vorks (C))			Destin	ation Networ	ks (1)	
▶ www URL	Search by name or v	alue				any					— 19	2.168.10.5/32		
😡 GeoLocation														0
💊 Variable Set	Networks		Geolocation											
SecurityIntelligence	Private Networks													
Sinkhole					Add to Source									
Cipher Suite List					Add to									
 International State International State<					Destination									
V Q PKI														
😑 Internal CAs														
🖶 Trusted CAs														
🖶 External Certs														
						Enter an IP a	ddress			Add	Enter	an IP address		Add
A Device Setup														
													Add	Cancel

Clique em Adicionar para adicionar a regra SSL.

Em seguida, clique em Store ASA Firepower Changes para salvar a configuração da política SSL.

Etapa 4. Configure a política de controle de acesso.

Depois de configurar a política SSL com regras apropriadas, você deve especificar a política SSL no Controle de Acesso para implementar as alterações.

Para configurar a política de controle de acesso, navegue para **Configuration > ASA Firepower Configuration > Policies > Access Control.**

Clique na opção **Nenhum** ao lado de **Política SSL** ou navegue para **Avançado > Configuração de política SSL**, especifique a política SSL na lista suspensa e clique em **OK** para salvá-la.

Clique em Armazene as alterações do ASA Firepower para salvar a configuração da política SSL.

Você deve implantar a política de controle de acesso. Antes de aplicar a política, você pode ver uma indicação Política de controle de acesso desatualizada no módulo. Para implantar as alterações no sensor, clique em **Implantar** e escolha a **opção Implantar alterações do FirePOWER.** Verifique as alterações feitas e clique em **Implantar** na janela pop-up.

Note: Na versão 5.4.x, se precisar aplicar a política de acesso ao sensor, clique em **Aplicar alterações do ASA FirePOWER**.

Note: Navegue até **Monitoring > ASA Firepower Monitoring > Task Status.** Em seguida, você se inscreve para alterações de configuração para garantir que a tarefa seja concluída.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

 Para a conexão SSL de saída, quando você navega em um site SSL público da rede interna, o sistema solicita uma mensagem de erro do certificado. Verifique o conteúdo do certificado e verifique as informações da AC. O certificado CA interno configurado no módulo Firepower é exibido. Aceite a mensagem de erro para navegar no certificado SSL. Para evitar a mensagem de erro, adicione o certificado CA à lista de CAs confiáveis do navegador.

C Q Search

х

Certificate Viewer:"www.cisco.com"

<u>G</u>eneral <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

 Verifique os eventos de conexão para verificar qual política SSL e regra SSL são atingidas pelo tráfego. Navegue até Monitoring > ASA FirePOWER Monitoring > Real-Time Eventing.Selecione um evento e clique em View Details. Verifique as estatísticas de descriptografia de SSL.

All ASA	FirePOWER Events Connect	on Intrusion File Malwa	re File Security Intelligence			
Filter	Connection Event Alle 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		https://sizes.kees.sizes.com/	Earess Interface	outside
	Autoritedulori Required	URL Catagoni	nttps://cisco-tags.cisco.com /	TCP Flags	0	
6/7/16	Transaction		URL Category	Pick unknown	NetBIOS Domain	not available
6/7/16	Initiator Packets	4.0	HTTP Response	0		
0/7/10	Responder Packets	9.0		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
6/7/16	Firewall Policy Rule/SI	Intrusion_detection	Client Tag	SSL protocol	SSL Rule	Outboound_SSL_Decrypt
0///10	Monitor Pules	not available	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	
	Converte Crown Too	pot available	Application Business	Medium	SSL Flow Error	Success

- Certifique-se de que a implantação da política de controle de acesso seja concluída com êxito.
- Certifique-se de que a política SSL esteja incluída na política de controle de acesso.
- Assegure-se de que a política SSL contenha regras apropriadas para as direções de Entrada e Saída.
- Certifique-se de que as regras SSL contêm a condição adequada para definir o tráfego interessante.
- Monitorar os eventos de ligação para verificar a política SSL e a regra SSL.
- Verifique o status da descriptografia SSL.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

Suporte Técnico e Documentação - Cisco Systems