ASDM(On-Box Management)を使用した FirePOWER モジュール上での SSL 復号化を設 定する

内容

概要 前提条件 要件 使用するコンポーネント 背景説明 アウトバウンドSSL復号化 着信SSL復号化 SSL復号化の設定 アウトバウンドSSL復号化(復号化 – 再署名) ステップ1:CA証明書を設定します。 ステップ2:SSLポリシーを設定します。 ステップ 3: 着信SSL復号化(復号化 – 既知) ステップ1:サーバ証明書とキーをインポートします。 ステップ2:CA証明書をインポートします(オプション)。 ステップ3:SSLポリシーを設定します。 ステップ4:アクセスコントロールポリシーを設定する。 確認 トラブルシュート 関連情報

概要

このドキュメントでは、ASDM(オンボックス管理)を使用した FirePOWER モジュールでのセ キュア ソケット レイヤ(SSL)復号の設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ASA(適応型セキュリティ アプライアンス)ファイアウォール、ASDM(Adaptive Security Device Manager)。
- FirePOWERアプライアンスに関する知識
- HTTPS/SSLプロトコルに関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェアバージョン6.0.0以降を実行するASA FirePOWERモジュール(ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)
- ソフトウェア バージョン 6.0.0 以降が稼働する ASA FirePOWER モジュール(ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

注:この機能を設定するには、FirePOWERモジュールに**保護ラ**イセンスがあることを確認 します。ライセンスを確認するには、[Configuration] > [ASA FirePOWER Configuration] > [License] に移動します。

背景説明

Firepowerモジュールは、それにリダイレクトされる着信および発信SSL接続を復号化して検査し ます。トラフィックが復号化されると、Facebookチャットなどのトンネルアプリケーションが検 出され、制御されます。復号化されたデータは、脅威、URLフィルタリング、ファイルブロッキ ング、または悪意のあるデータがないか検査されます。

アウトバウンドSSL復号化

firepowerモジュールは、発信SSL要求を傍受し、ユーザがアクセスするサイトの証明書を再生成 することによって、発信SSL接続の転送プロキシとして機能します。発行機関(CA)は、 Firepower自己署名証明書です。Firepowerの証明書が存在する階層の一部でない場合、またはク ライアントのブラウザキャッシュに追加されていない場合、クライアントはセキュアなサイトを ブラウズするときに警告を受信します。Decrypt-Resign方式は、発信SSL復号化を実行するため に使用されます。

着信SSL復号化

内部Webサーバまたは内部デバイスへの着信トラフィックの場合、管理者は保護されたサーバの 証明書とキーのコピーをインポートします。SSLサーバ証明書がFirepowerモジュールにロードさ れ、着信トラフィックに対してSSL復号化ポリシーが設定されると、デバイスはトラフィックを 復号化し、トラフィックの転送時にトラフィックを検査します。このモジュールは、悪意のある コンテンツ、脅威、このセキュアチャネルを通過するマルウェアを検出します。さらに、着信 SSL復号化を実行するためにDecrypt-Known Keyメソッドが使用されます。

SSL復号化の設定

SSLトラフィックの復号化には2つの方法があります。

- 復号化:アウトバウンドSSLトラフィックに対して再署名
- •復号化:着信SSLトラフィックで既知

アウトバウンドSSL復号化(復号化-再署名)

Firepowerモジュールは、パブリックSSLサーバのSSLネゴシエーションでMITM(man-in-themiddle)として機能します。Firepowerモジュールに設定されている中間CA証明書を使用して、パ ブリックサーバの証明書に再サインします。

アウトバウンドSSL復号化を設定する3つの手順を次に示します。

ステップ1:CA証明書を設定します。

自己署名証明書または中間の信頼できるCA証明書を証明書署名用に設定します。

自己署名CA証明書の設定

自己署名CA証明書を設定するには、[Configuration] > [ASA Firepower Configuration] > [Object Management] > [PKI] > [Internal CAs]に移動し、[Generate CA]をクリックします。CA証明書の詳 細を求めるプロンプトが表示されます。図に示すように、要件に従って詳細を入力します。

ASA FirePOWER Configur 🗗 🗜	Configuration > ASA FirePOWER Configuration > Object Management > PKI > Internal	I CAs
ASA FirePOWER Configur D Network Network Network Port Security Zones Application Filters URL GeoLocation Variable Set SecurityIntelligence Sinkhole FileList Cipher Suite List Distinguished Name PKI FileList Distinguished Name PKI External Certs Trusted CAs Finternal CAS Trusted CAs External Certs Finternal Certs Finternal CA Groups External Cert Groups External Cert Groups External Cert Groups Firewall Pevice Setup Perice Setup	Configuration > Object Management > PKI > Internal Image: Generate Internal Certificate Authority Name: ServerCA Country Name (two-letter code): IN State or Province: KA Locality or City: Bangalore Organization: TAC Organizational Unit (Department): TAC Common Name: serverCA.example.com	CAS A O Import CA ? × d CA Cancel
Firewall Remote Access VPN Site-to-Site VPN ASA FirePOWER Configuration	Generate CSR Generate self-signe	ed CA Cancel

[Generate self-signed CA]をク**リックして、内部CA**証明書を生成します。次に、[Generate CSR]をクリックして、証明書署名要求を生成します。これにより、署名するCAサーバと共有されます。

中間CA証明書の設定

別のサードパーティCAによって署名された中間CA証明書を設定するには、[Configuration] > [ASA Firepower Configuration] > [Object Management] > [PKI] > [Internal CAs]に移動し、[Import CA]をクリックします。

証明書の名前を指定します。[参**照]を選択**し、ローカルマシンから証明書をアップロードするか、 [証明書データ]オプションに証明書の内容をコピーア**ップし**ます。証明書の秘密キーを指定するに は、キーファイルを参照するか、[キー]オプションにキーをコピーペースト**し**ま**す**。

キーが暗号化されている場合は、[暗号化]チェックボックスをオン**にし**、パスワードを指定します。[OK]をクリックして、証明書の内容を保存します(図を参照)。

Configuration > ASA FirePOWE	<u>R Configuration > Object Management</u> > <u>PKI</u> > <u>Internal CAs</u>	
ASA FirePOWER Configuration 🗉		
	C Country Ch	C Januart CA
	Generate CA	
Port Port	Import Internal Certificate Authority Name: Intermediate-CA Certificate Data or, choose a file: Browse CBMCS0ExEjAQBgNVBAcTCUJBTkdBTE9SRTEOMAwGA1UEChMFQ01TQ08xDDAKBgNV BASTA1RBQzEaMBgGA1UEAxMRQ0Euc2VydmVydGVzdC5jb20xIzAhBgkqhkiG9w0B CQEWFGFkbWluQHNlcnZlcnRlc3QuY29tggkA90flOUfXIF0wDAYDVR0TBAUwAwEB /zANBgkqhkiG9w0BAQUFAA0BgQCXQME24zt0sKTzghQ15HuNWQl7NQlK3Zs5juVF YY24BJinUUIWSmCAID1KSyG+Jx26QlbWRs4vwfl8Fq3Dct0kRg74Qp0ZZS8l83F9 kuIpr+e7T+QifHbG4AzF5b2WGF4HUCXXjYTKtVHwbLuNeED5cAB38iL7Vso0cvq2	? ×
Internal CAS Trusted CAs External Certs Internal Certs Market Solution Internal CA Groups	Biat1w== END CERTIFICATE Key or, choose a file: Browse	×
Trusted CA Groups Internal Cert Groups Evternal Cert Groups III Device Setup	i/DnuBs9S3UgPnN3xShcwMTg8N+1yWOTJnfIpar/0LpW4Eqn5izAEAcTzNmA4gR/ 3XMIL1RbCFUpUyL9D2N+4TuZzHrbmUa6QA1qPNwLcf0Vf1wgVyagZYYAn5oA50wA K554gAeIyYJC5dEXe9974K9nh7/hNG5B53S3gKuGGvQx+0DSilZy000RPzRnQmew cNsbTQ3TGcdt6p58cJFsTWYZayvvQCbeJHOgNcGOUcfdlZ2/v6IoVC0wp+61KgZ7 jIgYPD5KzjJ5AX9BRKFXbsSAFJ3bSZ9Ztx/jFlvaMdjEUqqctEPP69Fav6zSdTDo wFkMModFPeSBol7WLTjKujyRLM0/p7DsM41Wdn4x1J2j2k+E9AWoXw+kGF9PwNBQ	•
Firewall	22WYRn92UiZWTKySdU0Mr4mDRVBkzb+Iqb30D7/S7ENWFpuktxWOQA== END RSA PRIVATE KEY	
Remote Access VPN Image: Site-to-Site VPN	Encrypted, and the password is:	<u> </u>
ASA FirePOWER Configuration	ок	Cancel

ステップ2:SSLポリシーを設定します。

SSLポリシーは、復号化アクションを定義し、復号化のDecrypt-Resign方式が適用されるトラフィックを識別します。ビジネス要件と組織のセキュリティポリシーに基づいて、複数のSSLルールを設定します。

SSLポリシーを設定するには、[Configure] > [ASA FirePOWER Configuration] > [Policies] > [SSL]に移動し、[Add Rule]をクリックします。

名前:ルールの名前を指定します。

アクション:アクションをDecrypt - Resignと指定し、前の手順で設定したドロップダウンリストからCA証明書を選択します。

復号化が必要なトラフィックを定義するために指定された複数のオプション(ゾーン、ネットワ ーク、ユーザなど)があるため、トラフィックを照合するルールの条件を定義します。 SSL復号化のイベントを生成するには、次の図に示すように、ログ**記録オ**プションを有効にしま す。

○ ○ ○ ASA FirePOWER Configurat	○ ○ ○ <u>Configuration > ASA Fire</u>	POWER Configuration >	> Policies > SSL				
Policies Access Control Policy	Default SSL Policy						
► 💿 Intrusion Policy	SSL Policy						
Files							
Lidentity Policy	Rules Trusted CA Certificates	Undecryptable Actions	ן				FC (LA
DNS Policy		,,,			Add Category	Add Rule Search Rules	×
Device Management Object Management Imagement							
 A Local 	Add Rule						? ×
System Information	Name Outboound SSL Decrypt		C Enabl	ed In	sert into Category	Y Standar	rd Rules 🗸
Licenses	Action Community Design	with ConverCt			enlace Key		
Tools	Action Decrypt - Resign	ServerCA	·				
🕨 🍡 Integration	Zones Networks Users	Applications Ports	Category Certificate	DN Cert Status	Cipher Suite	Version	Logging
	Available Networks	0	Source Net	works (1)		Destination Networks (0)	
	Search by name or value		📻 Private I	Networks	i	any	
	Networks	Geolocation					
	Private Networks						
			Source				
			Add to				
			Destination				
Davica Satup				- dd		Talan an TB address	
			Enter an IP	aduress	Add	Enter an IP address	Add
Firewall						Add	Cancel
🥂 Remote Access VPN							
🔗 Site-to-Site VPN							
ASA FirePOWER Configur						No data to display 🛛 🗶 Pa	age 1 of 1 > > C

[Add]をクリックし、SSLルールを追加します。

[Store ASA Firepower Changes]をクリックして、SSLポリシーの設定を保存します。

ステップ 3:

適切なルールを使用してSSLポリシーを設定したら、変更を実装するためにアクセスコントロー ルでSSLポリシーを指定する必要があります。

アクセスコントロールポリシーを設定するには、[Configuration] > [ASA Firepower Configuration] > [Policies] > [Access Control]**に移動します。**

SSLポリシーの**[None]**をクリック**するか、[**Advanced] > [**SSL Policy Setting]に移動します。**次の 図に示すように、ドロップダウンリストからSSLポリシーを指定し**て**、[**OK**]をクリックして保存 します。

O O ASA FirePOWER Configurat	O O Configuration > ASA FirePOWER Configuration > Policies > Access (Control
▼ / Policies		
Access Control Policy	ASA ASA FirePOWER	
Intrusion Policy		
💾 Files	Default Allow All Traffic	
SSL SSL	Enter a description	
X Actions Alerts		
Lidentity Policy		
DNS Policy		
Device Management		
Object Management		
► Cal	Identity Policy: None SSL Policy: None	
Undates	Rules Security Intelligence HTTP Responses Advanced	
Licenses	Conoral Sattings	ß
Tools	General Settings	U
🕨 🍇 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 ? *	Yes
	connections	Voc
	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

クリック ASA Firepowerの変更の保存 SSLポリシーの設定を保存します。

アクセスコントロールポリシーをセンサーに展開する必要があります。ポリシーを適用する前に 、モジュール上のアクセスコントロールポリシーが古いことを示しています。センサーに変更を 展開するには、[Deploy]をクリックし、[Deploy FirePOWER Changes]オプションを選択してくだ さい。変更を確認し、[Deploy]をクリックします。

注:バージョン5.4.xで、アクセスポリシーをセンサーに適用する必要がある場合は、[Apply ASA FirePOWER Changes]をクリックします。

注: [Monitoring] > [ASA Firepower Monitoring] > [Task Status] に移動します。次に、設定変 更を適用して、タスクが完了したことを確認します。

着信SSL復号化(復号化 – 既知)

着信SSL復号化(Decrypt-Known)方式は、サーバ証明書と秘密キーを設定した着信SSLトラフィックを復号化するために使用されます。サーバ証明書と秘密キーをFirepowerモジュールにインポートする必要があります。SSLトラフィックがFirepowerモジュールにヒットすると、トラフィックが復号化され、復号化されたトラフィックに対する検査が実行されます。インスペクション後、Firepowerモジュールはトラフィックを再暗号化し、サーバに送信します。

アウトバウンドSSL復号化を設定する4つの手順を次に示します。

サーバ証明書とキーをインポートするには、[Configuration] > [ASA Firepower Configuration] > [Object Management] > [PKI] > [Internal Certs]に移動し、[Add Internal Cert]をクリックします。

図に示すように、証明書の名前を指定します。ローカルマシンから証明書を選択するか、証明書 データに証明書の内容をコピーアンドペーストする場合は、[参照]を選択します。証明書の秘密キ ーを指定するには、キーファイルを参照するか、キーをコピー&ペーストしてオプションKeyに貼 り付けま。

キーが暗号化されている場合は、図に示すように、[Encrypted]チェックボックス**をオン**にし、パ スワードを指定します。

O O ASA FirePOWER Configurat	O O Configuration > ASA FirePOWER Configuration > Object Management > PKI > Interna	l Certs
Application Filters		
► WWW URL	Add Internal Cert	🔍 Fi
😡 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	mjzrywuy4zi8u5z0r/9YnNJoz/212aVR4U21PA9AQqXvyeCCL/UCQmFQOrP6+qbk +FPHI f9wFxBahpFCAwFAATANBakahkiG9w0BAOsFAAQBaQCukZVPuTaileuiPrtF	
🖶 Trusted CAs	Lrcyns+lrbHTJhge0Z2HC/XJmYwyJXhBuEqvU9qx+GhQ99jNCOlo0iPIGF1naqBt	
🖶 External Certs	FtI7ohmI/F544x75fm17t3XwfZF/VA2GhG3W3QGFKHCA0U7CBaU78jCVBa9CTKOG	
🖶 Internal Certs	END CERTIFICATE	
👶 Internal CA Groups		
👶 Trusted CA Groups		
👶 Internal Cert Group:	Rey or, choose a file: Browse	
👶 External Cert Group		
🕨 🏠 Local	EccERsWn5JXOTtaTs+WN1d3+wHieG+9897aU3rki6s2aPNiLBTLiOLv5LM6v/1iE	
🛐 System Information	0mjP/YjZ29Hi5nU8D0BCpe/J4IIv84JCYVA6s/r6puT4U8ct/3AXEGCGkQIDAQAB	
📑 Updates	AoGBAJ+XOAu5cCAIhP6ujZZHzbjJEnNmQvGz2uiVh3HlsfY6SWxR87ic8zRROZBq	
🔛 Licenses	+nzEJwx4LgmXR8N88YbkvC3n4iVY5z90fsvCdJ2UoAGBXN4BAkEA+nkDe1UglxOz	
V 💼 Tools	Pgmzad68lngk4/7Wbg8ibZz0Mv2PSvO7pNbhRfpy/dtgGLJvIGJIr/+0iL2SrPFv	
🗑 Backup Restore	d7QmDkGwyQJBANeOlVWWjBPuFCLQjYL04c66km9vzGgLDHjGc4gOING1iFlCrQt1	
Cabadulina	Encrypted, and the password is:	
💑 <u>D</u> evice Setup		el

[Store ASA FirePOWER Changes]をクリックして、証明書の内容を保存します。

ステップ2:CA証明書をインポートします(オプション)。

内部の中間CA証明書またはルートCA証明書によって署名されたサーバ証明書の場合、CA証明書 の内部チェーンをFirepowerモジュールにインポートする必要があります。インポートの実行後、 firepowerモジュールはサーバ証明書を検証できます。

CA証明書をインポートするには、[Configuration] > [ASA Firepower Configuration] > [Object Management] > [Trusted CAs]に移動し、[Add Trusted CA]をクリックしてCA証明書を追加します。

ステップ3:SSLポリシーを設定します。

SSLポリシーは、着信トラフィックを復号化するDecrypt-known方式を設定するアクションとサーバの詳細を定義します。複数の内部サーバがある場合は、異なるサーバと、それらのサーバが処

理するトラフィックに基づいて、複数のSSLルールを設定します(SSLルールはSSLルールに基 づいて設定します)。

SSLポリシーを設定するには、[Configure] > [ASA FirePOWER Configuration] > [Policies] > [SSL]に移動し、[Add Rule]をクリックします。

名前:ルールの名前を指定します。

アクション:アクションとして**Decrypt - knownを指定**し、前の手順で設定したドロップダウンリ ストからCA証明書を選択します。

SSL復号化を有効にするサーバーの対象トラフィックを定義するために複数のオプション(ネットワーク、アプリケーション、ポートなど)が指定されているため、このルールに一致する条件を定義します。[信頼できるCA証明書]タブの[選択された信頼できるCA]で内部CAをををにします。

SSL復号化のイベントを生成するには、ロギング・オプションを有効にします。

○ ○ ○ ASA FirePOWER Configurat	O O O Configuration >	ASA FirePOWER Cor	figuration >	<u>Policies</u> > <u>SSL</u>				
V Dolicies								
Access Control Policy	Default SSL Pol	licy						
🔻 💿 Intrusion Policy								
Intrusion Policy	SSL POICY							
👼 Rule Editor								
🖺 Files								
🔒 SSL	Rules Trusted CA Cert	tificates Undecrypta	ble Actions					
🔯 Actions Alerts						0		
🚨 Identity Policy	Add Rule							? ×
DNS Policy								
🕨 🔜 Device Management	Name Web_Server_Decr	ypt		Enable	đ	Insert below rule	▼ 1	
🔻 🧒 Object Management								
Network	Action Decrypt - Know	wn Key 💙 With	web.servertes	st.com	Edit	•		
Port	Zanas Maturatia	Lisers Application	Douto C	Catagony	DN Cort Statu	Cinhan Cuita	Versien	Lagging
Security Zones	Zones Networks	Osers Application	is Ports C	Category	UN Cert Statu	s Ciprier Suite	version	Logging
Application Filters	Available Networks 🖒			Source Netw	orks (0)		Destination Networks (1)	
► www. URL	Search by name or valu	ue		any			2 192.168.10.5/32	
GeoLocation								
🤏 Variable Set	Networks	Geolocation						
SecurityIntelligence	Private Networks							
Sinkhole			4	Add to				
FileList								
😳 Cipher Suite List			A P	Add to				
Distinguished Name								
V SPRI								
🖶 Internal CAs								
H Trusted CAs								
😝 External Certs								
				Enter an IP a	ddress	Add	Enter an IP address	Add
A Device Setup								
								Add Cancel

[Add]をクリックし、SSLルールを追加します。

次に、[Store ASA Firepower Changes]をクリックし、SSLポリシーの設定を保存します。

ステップ4:アクセス コントロール ポリシーを設定する。

適切なルールを使用してSSLポリシーを設定したら、変更を実装するためにアクセスコントロー ルでSSLポリシーを指定する必要があります。

アクセスコントロールポリシーを設定するには、[Configuration] > [ASA Firepower Configuration] > [Policies] > [Access Control]**に移動します。**

[SSL Policy]の横にある[None]オプションをクリックするか、[Advanced] > [SSL Policy Setting]に 移動し、ドロップダウンリストからSSLポリシーを指定し、[OK]をクリックして保存します。

クリック ASA Firepowerの変更の保存 SSLポリシーの設定を保存します。

アクセス コントロール ポリシーを展開する必要があります。ポリシーを適用する前に、モジュー ルにAccess Control Policyの最新の情報が表示されます。センサーに変更を展開するには、 [Deploy]をクリックし、[Deploy FirePOWER Changes]オプションを選択します。変更を確認し、 ポップアップウィンドウで[Deploy]をクリックします。

注:バージョン5.4.xでは、アクセスポリシーをセンサーに適用する必要がある場合は、 [Apply ASA FirePOWER Changes]をクリックします。

注: [Monitoring] > [ASA Firepower Monitoring] > [Task Status] に移動します。次に、設定変 更を適用して、タスクが完了したことを確認します。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

 アウトバウンドSSL接続では、内部ネットワークからパブリックSSL Webサイトを参照する と、システムから証明書のエラーメッセージが表示されます。証明書の内容を確認し、CA情報を確認します。Firepowerモジュールで設定した内部CA証明書が表示されます。エラーメ ッセージを受け入れて、SSL証明書を参照します。エラーメッセージが表示されないように するには、ブラウザの信頼できるCAリストにCA証明書を追加します。

ficate Viewer:"www.ciso	o.com"	
neral <u>D</u> etails		
Could not verify this c	ertificate because the issuer is unknown.	
Issued To		
Common Name (CN)	www.cisco.com	
Organization (O)	Cisco Systems	
Organizational Unit (Ol	J) ATS	
Serial Number	14:5E:8D:FB:06:DA:C6:55	
Issued By		
Common Name (CN)	serverCA.example.com	
Organization (O)	TAC	
Organizational Unit (Ol	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	

• 接続イベントをチェックして、トラフィックによって中断されているSSLポリシーとSSLル

ールを確認します。[Monitoring] > [ASA FirePOWER Monitoring] > [Real-Time Eventing]に移 動します。イベントを選択し、[View Details]をクリックします。SSL復号化の統計情報を確 認します。

ime Eventi	ing					
All ASA	A FirePOWER Events Connect	tion Intrusion File Malwa	re File Security Intelligence			
ilter	Connection Event All	ow		Time: Wed 6/7/16 6	:29:10 AM (IST) to	Wed 6/7/16 6:29:11 AM (IST)
	ASA FirePOWER firewall connect	ction event				
	Reason:					
🕨 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
0/7/10	Source Port/ICMP Type	56715	Destination Port/ICMP	443	Zone	
6/7/16	User	Special Identities/No	Code		Ingress Interface	inside
	Authentication Required	URL	https://cisco-tags.cisco.com /	Egress Interface	outside	
6/7/16	Transaction		URL Category	not available	NotBIOS Domain	0 not susibble
	Initiator Packets	4.0	URL Reputation	Risk unknown	NetBIOS Domain	not available
6/7/16	Responder Packets	9.0	HTTP Response	U	DNS	
6/7/16	Total Packets	13.0	Application		DNS Query	not available
0/7/10	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
0/7/10	Monitor Rules	not available	Web Application	Cisco	SSL Version	TLSVI.U
6/7/16	- Ionicor Adico	100 0101000	Web App Categories	web services provider	SSL Cipher Suite	_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

- アクセス コントロール ポリシーの導入が正常に完了したことを確認します。
- アクセスコントロールポリシーにSSLポリシーが含まれていることを確認します。
- SSLポリシーに、インバウンド方向とアウトバウンド方向の適切なルールが含まれていることを確認します。
- SSLルールに、対象トラフィックを定義する適切な条件が含まれていることを確認します。
- 接続イベントを監視して、SSLポリシーとSSLルールを確認します。
- •SSL復号化ステータスを確認します。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

・ <u>テクニカル サポートとドキュメント – Cisco Systems</u>