

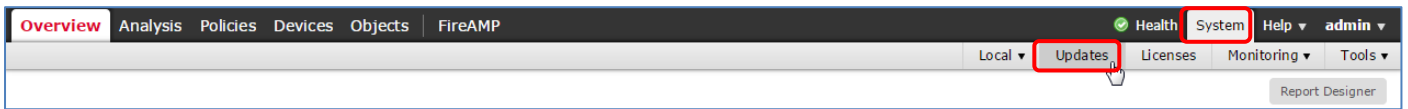
# SRU (Sourcefire Rule Update) インストール方法

2015/02/15

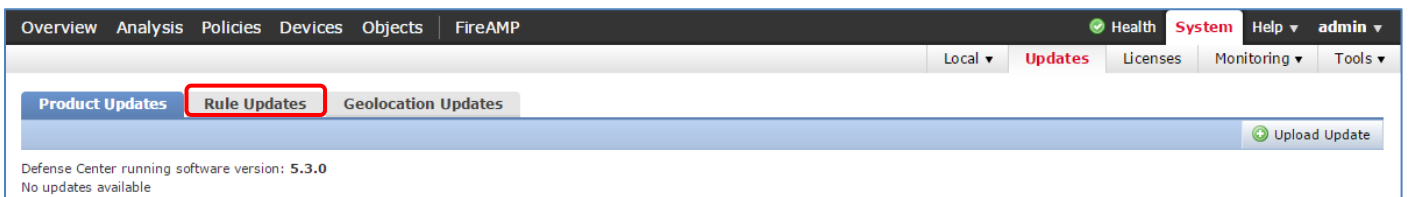
Rev1.0

FireSight(Defense Center) 上にて、手動での SRU(Sourcefire Rule Update) のアップデート方法をご紹介します。FirePower については、FireSight 上でアップデートを実施した後に FireSight から FirePower に新しい SRU 情報をアップデートします。FirePower の SRU アップデートについては本ドキュメント中で説明いたします。

FireSight の GUI にログインします。(https://<FireSight IP アドレス>)  
トップ画面から、System -> Updates に移動します。

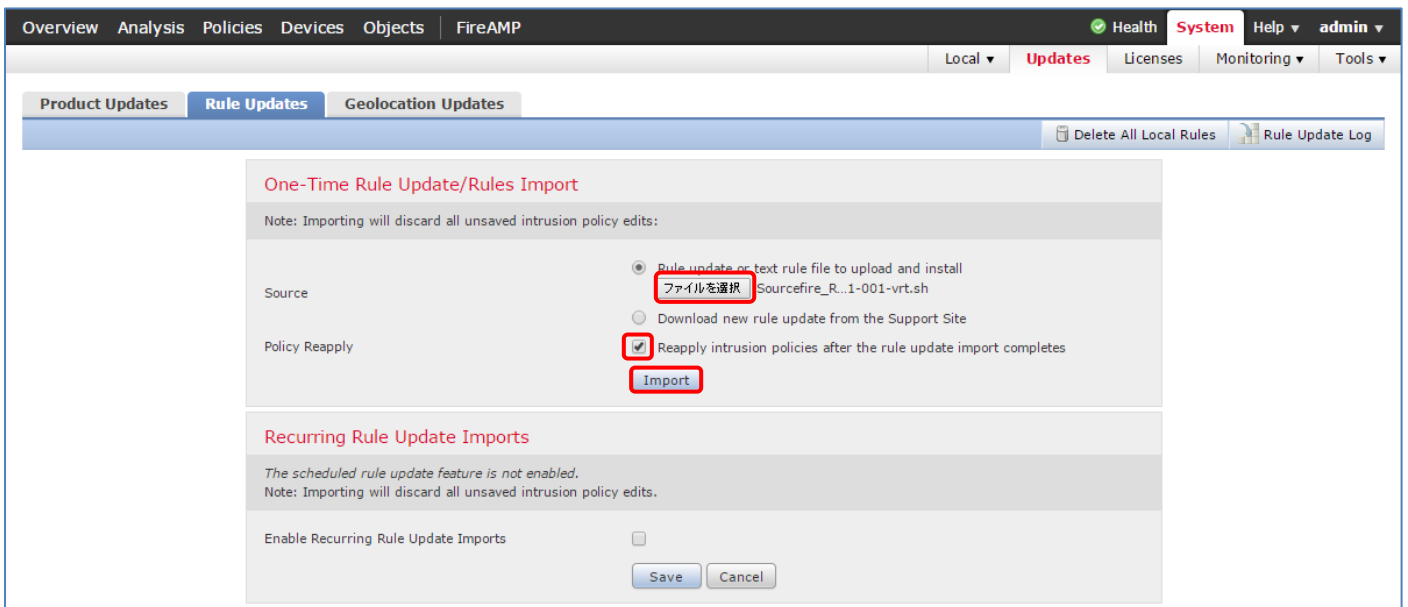


Rule Updates タブをクリックします。



- ・ファイルを選択 ボタンをクリックして、適応したい SRU を選択する。(PC 上に SRU ファイルがある必要があります)
- ・(オプション)Policy intrusion policies after the rule update import completes のチェックボックスにチェックして、FirePower に新しい SRU 情報を FS に適用後に、適用します。※1
- ・Import ボタンを押して、SRU 情報をアップデートします。

※数分の間、この画面で止まっている状態となります。



数分後、以下のような新しいルールの一覧が自動的に表示されます。

以上で、FS への SRU アップデートは完了です。本画面が表示されると、自動的に FirePower へ新しい SRU のアップデートが開始されます。


The screenshot shows the 'Rule Update Import Log' table in the FireAMP interface. The table lists various rule updates with columns for Time, Name, Type, Action, Default Action, GID, SID, Rev, Policy, Details, and Count. The 'Status' column is not visible in this view.

Time	Name	Type	Action	Default Action	GID	SID	Rev	Policy	Details	Count
2015-02-12 09:38:15	DCE2_EVENT SMB_CHAIN_TC_TDIS	rule	new	Alert	133	24	1	All	New	1
2015-02-12 09:38:15	DCE2_EVENT SMB_CHAIN_OPEN_CLOSE	rule	new	Alert	133	25	1	All	New	1
2015-02-12 09:38:15	DCE2_EVENT SMB_INVALID_SHARE	rule	new	Alert	133	26	1	All	New	1
2015-02-12 09:38:15	DCE2_EVENT CO_BAD_MAJ_VERSION	rule	new	Alert	133	27	1	All	New	1
2015-02-12 09:38:15	DCE2_EVENT CO_BAD_MIN_VERSION	rule	new	Alert	133	28	1	All	New	1
2015-02-12 09:38:15	DCE2_EVENT CO_BAD_PDU_TYPE	rule	new	Alert	133	29	1	All	New	1
2015-02-12 09:38:15	DCE2_EVENT CO_FLEN_LT_HDR	rule	new	Alert	133	30	1	All	New	1
2015-02-12 09:38:15	DCE2_EVENT CO_FLEN_LT_SIZE	rule	new	Alert	133	31	1	All	New	1
2015-02-12 09:38:15	DCE2_EVENT CO_ZERO_CTX_ITEMS	rule	new	Alert	133	32	1	All	New	1
2015-02-12 09:38:15	DCE2_EVENT CO_ZERO_TSYNS	rule	new	Alert	133	33	1	All	New	1
2015-02-12 09:38:15	DCE2_EVENT CO_FRAG_LT_MAX_XMIT_FRAG	rule	new	Alert	133	34	1	All	New	1
2015-02-12 09:38:15	DCE2_EVENT CO_FRAG_GT_MAX_XMIT_FRAG	rule	new	Alert	133	35	1	All	New	1
2015-02-12 09:38:15	DCE2_EVENT CO_ALTER_CHANGE_BYTE_ORDER	rule	new	Alert	133	36	1	All	New	1
2015-02-12 09:38:15	DCE2_EVENT CO_FRAG_DIFF_CALL_ID	rule	new	Alert	133	37	1	All	New	1
2015-02-12 09:38:15	DCE2_EVENT CO_FRAG_DIFF_OPNUM	rule	new	Alert	133	38	1	All	New	1
2015-02-12 09:38:15	DCE2_EVENT CO_FRAG_DIFF_CTX_ID	rule	new	Alert	133	39	1	All	New	1




FireSight 上への SRU 更新完了確認方法

System > Updates > Rule Updates 上の Rule Update Log ボタンをクリックする。

The screenshot shows the 'Rule Updates' page in the FireAMP interface. The 'Rule Update Log' button is highlighted with a red box.

適応した SRU が表示され、Status が  になっていることを確認する。

The screenshot shows the 'Rule Update Log' table in the FireAMP interface. The table lists various rule updates with columns for Summary, Time, User ID, and Status. The 'Status' column shows green checkmarks for completed updates.

Summary	Time	User ID	Status
Sourcefire Rule Update 2013 12 11 001 vrt Completed install of Sourcefire Rule Update 2013-12-11-001-vrt	2015-02-12 09:34:36	admin	
Sourcefire Rule Update 2014 12 03 001 vrt Completed install of Sourcefire Rule Update 2014-12-03-001-vrt	2015-02-12 01:40:00	admin	
Sourcefire Rule Update 2014 12 01 001 vrt Completed install of Sourcefire Rule Update 2014-12-01-001-vrt	2015-02-12 01:34:16	admin	

※1


(オプション)Policy intrusion policies after the rule update import completes のチェックボックスでチェックしなかった場合には、FireSight の SRU 適応が完了しても自動的に FirePower には適応しません。

完了後、FireSight の Policy > Access Control のページに移動すると Access Control policy out-of-date on xx devices というメッセージが表示されます。これは、FireSight と FirePower の SRU バージョンが違う際に表示されます。

※これ以前に、Access Control Policy を変更している場合には、SRU 以外の他の変更点がある場合があります。

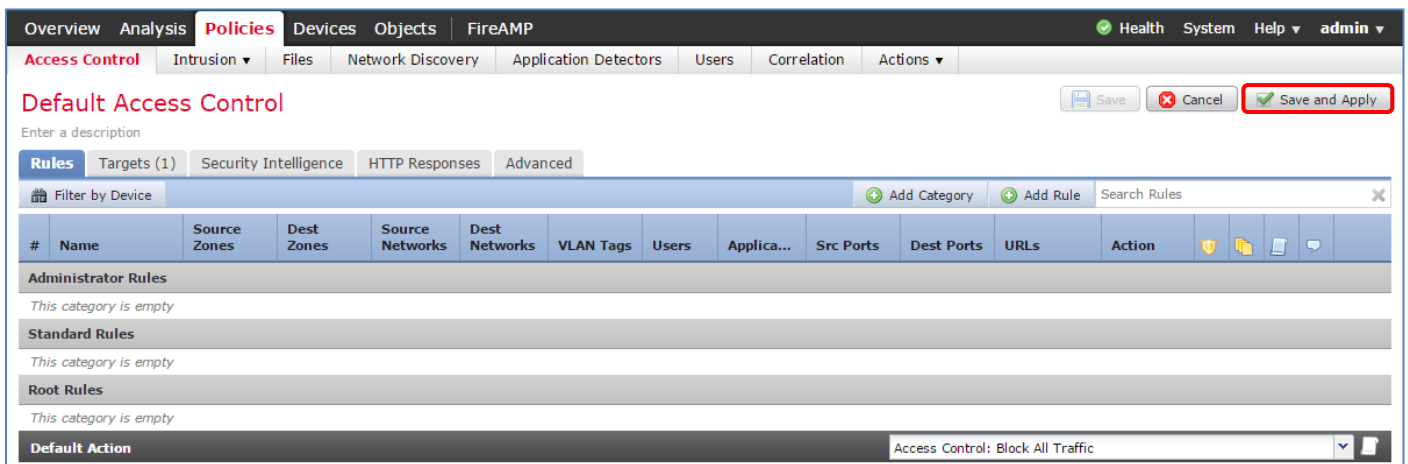


FirePower にも新しい SRU を適用するには

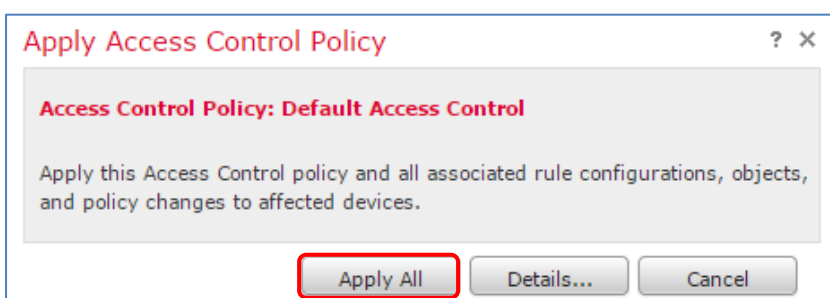
Access Control policy out-of-date on xx devices メッセージの右側にある  ボタンをクリックする。



Save and Apply ボタンをクリックする。



Apply All ボタンを押すと、新しいポリシー(新しいSRU)を FirePower に適用します。



以上