ISR4000シリーズ Snort インストールガイド

Released: Mar, 2016

はじめに

- 本ガイドは、Cisco ISR4000シリーズのサービスコンテナ上でサポートする SNORT のインストールガイドとなります。

  米国シスコ発行ドキュメントを参考和訳し、内容をまとめた資料です。
  リンク情報につきましては、リンク先のページが移動/変更されている場合がありますことをご了承ください。
  (リンク情報はスライド13ページに記載)
  英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

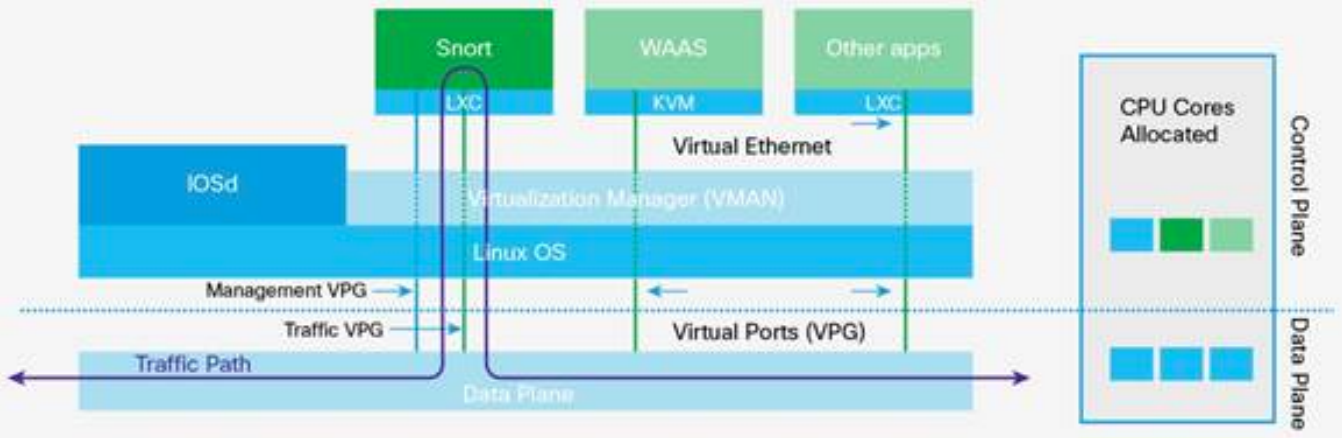
ライセンス および サポートモデルについて

- IPSエンジンは追加料金無しでSEC licensesに含まれます。
- 2種類の Snort Rule Set :
  - Snort community rule set (無料) – 1年
  - Snort subscriber rule set – 1年
  - Snort subscriber rule set – 3年

注意 Snortルールセットはcisco.com提供のもの
のみサポートします。
snort.org提供のものはサポートされません。

	Community Rule Set	Subscriber Rule Set
価格	無償	有償
ルールの数	3000+	30000+
Coverage in advance of exploits	なし	あり
シグニチャーの有効化	30日後	最新版に即座にアップデート
SLA	なし	
TACサポート	なし	Bug Fix のみ (L3)

Snort Overview



Snort ISR4000アーキテクチャ概要
-Snort：オープンソースのIPSエンジン
-このエンジンをISR4000内のLinuxContainer(LXC)上のアプリケーションとして実行。
-ISR4000のIOS-XEではマルチコアCPUを使用し制御プレーン/データプレーンを各コアに割当てる
Snortエンジンはデータプレーンと分離して実行が可能
-ルータ内部では、仮想ポートグループ(VPG)インターフェースを使用してSnortコンテナにパケットを転送
-VPGインターフェースはルータのバックプレーンを介して接続されている
-IPS上でパケットを検査し、Bad Flowは廃棄、Good Flowはルータへリターンされる

Snort インストール サマリー

- Step 1 OVA ファイルのコピー
- Step 2 Snort OVA のインストール
- Step 3 VPGインターフェースの作成
- Step 4 IPS Virtual Service の作成と Activate

Snort インストールガイド Step 0

- IOS-XEでのSnortコンテナ サポートVersionは 3.16.1S/3.17S～
- 物理メモリ 最少8GB必要 (満たさない場合インストール不可)
  物理メモリが4GBの場合、後述の virtual-service install コマンドが表示されません。
  搭載されている物理メモリサイズは show version コマンドを実行して確認します。

```
ISR4331#show version
Cisco IOS XE Software, Version 03.17.00.S - Standard Support Release
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 15.6(1)S, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 25-Nov-15 14:33 by mcpre

=== 省略 ===

cisco ISR4331/K9 (1RU) processor with 7797212K/6147K bytes of memory.
Processor board ID FDO1850A03W
3 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
16777216K  bytes of physical memory.
14659583K bytes of flash memory at bootflash:.


Configuration register is 0x2102


ISR4331#
```

16GBメモリが搭載されているケース

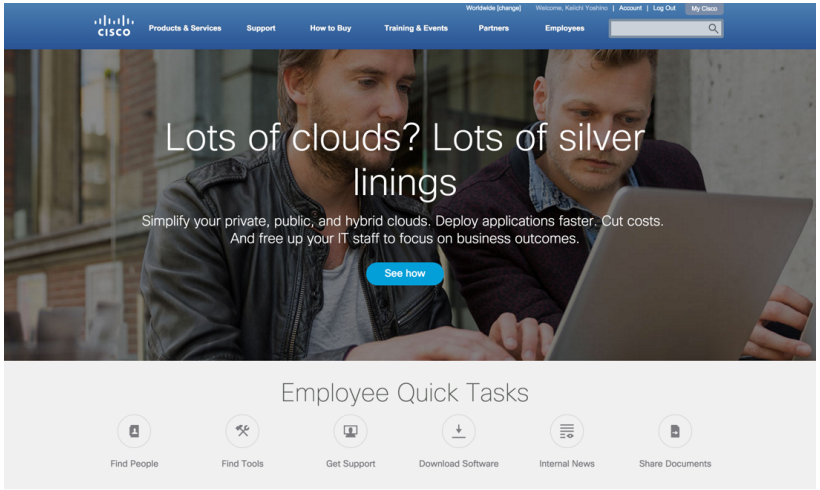
Snort インストールガイド Step 1

- Snortの仮想コンテナサービスをインストール
  サービスコンテナで実行されるSnortエンジンはOpen　Virtual Archive (OVA) として配布されています
- ルータのFlashにOVAファイルをコピーします
- OVAファイルはCisco.comのソフトウェアダウンロードサイトから入手可能です　(※下記URL参照)
  http://www.cisco.com/c/en/us/products/collateral/security/router-security/guide-c07-736629.html#_Toc442352491
- Snort IPS OVAはIOS-XEと互換性のあるOVAをダウンロードします。

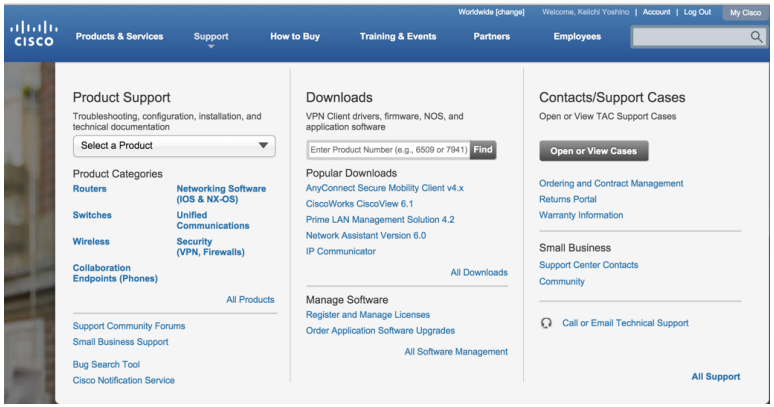
```
ISR4331#dir
Directory of bootflash:/


  11  drwx         16384   Dec 12 2014 20:15:20 +00:00  lost+found
1163265  drwx          4096   Mar 4 2016 07:12:20 +00:00  .prst_sync
  12  -rw-       470602752   Feb 25 2016 06:50:54 +00:00  isr4300-universalk9.03.16.02.S.155-3.S2-ext.SPA.bin
1736705  drwx          4096   Dec 12 2014 20:15:56 +00:00  .installer
1114113  drwx          4096   Nov 17 2015 06:30:26 +00:00  core
65537  drwx          4096   Dec 12 2014 20:34:39 +00:00  .rollback_timer
49153  -rw-             0   Dec 12 2014 20:34:55 +00:00  tracelogs.498
999425  drwx         57344   Mar 4 2016 07:22:08 +00:00  tracelogs
  13  -rw-          2991   Feb 25 2016 11:40:28 +00:00  g09-isr4331-01-confg_2
114689  drwx          4096   Nov 17 2015 06:29:52 +00:00  virtual-instance
49155  -rw-            30   Mar 4 2016 07:12:20 +00:00  throughput_monitor_params
49156  -rw-          2199   Jan 6 2016 08:52:38 +00:00  FOC17042FM4_201601060033280070.lic
49157  -rw-          1976   Jan 7 2016 01:57:07 +00:00  ipsec-orig.cfg
49158  -rw-          3499   Jan 12 2016 01:09:16 +00:00  dmvpn.cfg
  14  -rw-          1363   Feb 26 2016 09:34:24 +00:00  PnP-cert_09_34_24_UTC_Fri_Feb_26_2016.ca
49160  -rw-          2298   Feb 23 2016 07:33:57 +00:00  isr4331_20160223
49161  -rw-          2233   Feb 24 2016 06:04:18 +00:00  isr4331_20160224
  15  -rw-     473921888   Mar 4 2016 07:06:16 +00:00  isr4300-universalk9.03.17.00.S.156-1.S-std.SPA.bin
  16  -rw-     209950720   Mar 4 2016 07:28:55 +00:00  iosxe-utd-ips.03.17.00.S.156-1.S-std.1_1_0_SV2975.ova


14775529472  bytes total (12861235200  bytes free)
```

Cisco.com からのソフトウェアダウンロード方法

① Cisco.comにアクセスします



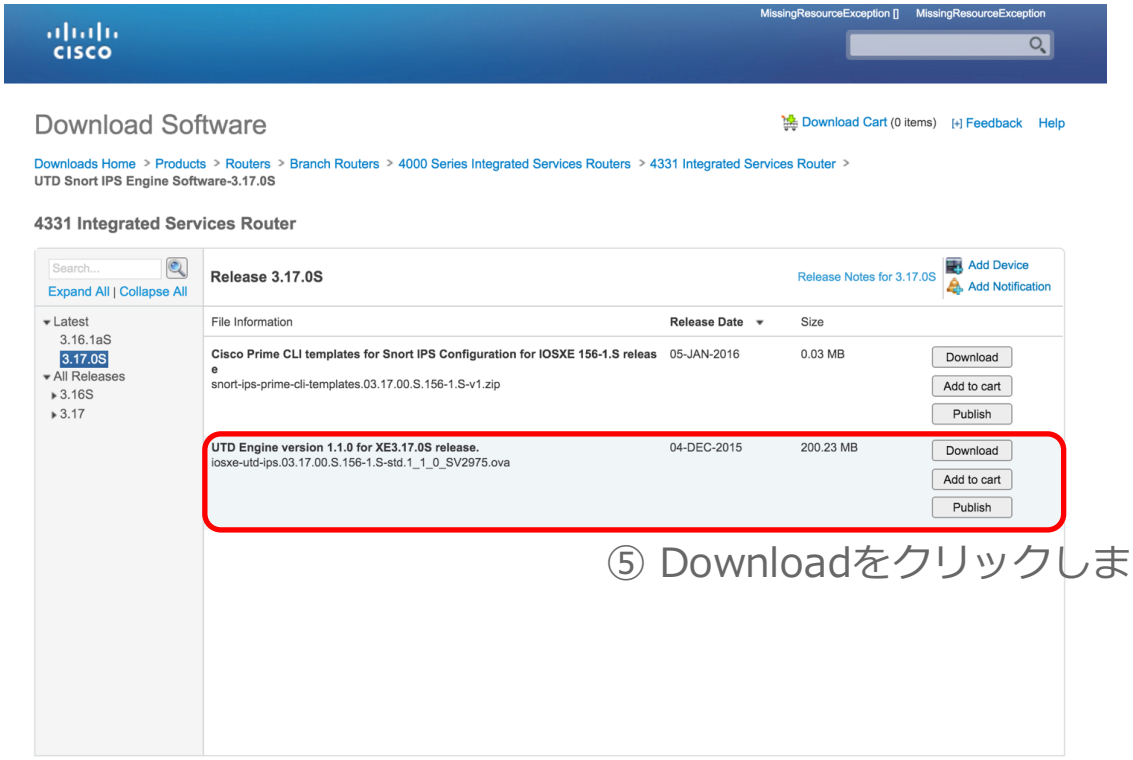
② Support をポイントしRoutersを選択します



③ 下記の通りリンクをたどります

Downloads Home > Products > Routers > Branch Routers > 4000 Series Integrated Services Routers
> 4331 Integrated Services Router > UTD Snort IPS Engine Software

④ ISR4331の UTD Snort IPS Engine Software 選択した画面



⑤ Downloadをクリックします

Snort インストールガイド Step 2

- 下記コマンドをExecモードで実行しOVAファイルをインストールします
- show virtual-service list コマンドで Installation Statusを確認可能です

```
ISR4331#virtual-service install name SNORT package flash:iosxe-utd-ips.03.17.00.S.156-1.S-std.1_1_0_SV2975.ova

Installing package 'bootflash:/iosxe-utd-ips.03.17.00.S.156-1.S-std.1_1_0_SV2975.ova'   for virtual-service 'SNORT'. Once the install has
finished, the VM may be activated. Use 'show virtual-service list' for progress.


ISR4331#
*Mar  4 07:52:17.119:  %VMAN-5-PACKAGE_SIGNING_LEVEL_ON_INSTALL: SIP1: vman:  Package 'iosxe-utd-ips.03.17.00.S.156-1.S-
std.1_1_0_SV2975.ova'   for service container 'SNORT' is 'Cisco signed', signing level cached on original install is 'Cisco signed'
*Mar  4 07:52:19.001:  %VIRT_SERVICE-5-INSTALL_STATE:  Successfully installed virtual service SNORT
*Mar  4 07:52:19.079:  %ONEP_BASE-6-SS_ENABLED:  ONEP: Service set Base was enabled by  Default
ISR4331#
ISR4331#
ISR4331#
ISR4331#sh virtual-service list
Virtual Service List:



Name                 Status           Package Name
------------------------------------------------------------------------------
SNORT                 Installed        iosxe-utd-ips.03.17.00.S.156-1.S...
```

Snort インストールガイド Step 3

- VPG (Virtual Port Group) インターフェースの作成
  管理用インターフェースおよびデータ用インターフェースの2つを作成します
  (管理用インターフェースはVPGもしくはオプションでGig0を選択可能)
  一つ目のVPGは管理用インターフェースとなり、シグニチャの更新、ロギング、監視に使用します
  二つ目のVPGはIOSデータプレーンとSnort IPS間のパケット転送に使用されます

```
ISR4331#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISR4331(config)#interface VirtualPortGroup0
ISR4331(config-if)#ip address 10.255.255.1 255.255.255.252
ISR4331(config-if)#interface VirtualPortGroup1
ISR4331(config-if)#ip address 192.168.0.1 255.255.255.252
ISR4331(config-if)#
ISR4331(config-if)#^Z
ISR4331#
```

```
ISR4331#sh run int vir0
Building configuration...


Current configuration : 106 bytes
!
interface VirtualPortGroup0
 ip address 10.255.255.1 255.255.255.252
 no mop enabled
 no mop sysid
end


ISR4331#sh run int vir1
Building configuration...


Current configuration : 105 bytes
!
interface VirtualPortGroup1
 ip address 192.168.0.1 255.255.255.252
 no mop enabled
 no mop sysid
end
```

Snort インストールガイド Step 4

- IPS Virtual Service の作成と Activate

```
ISR4331#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ISR4331(config)#virtual-service SNORT
ISR4331(config-virt-serv)#vnic gateway virtualPortGroup 0
ISR4331(config-virt-serv-vnic)#guest ip address 10.255.255.2
ISR4331(config-virt-serv-vnic)#exit
ISR4331(config-virt-serv)#vnic gateway virtualPortGroup 1
ISR4331(config-virt-serv-vnic)#guest ip address 192.168.0.2
ISR4331(config-virt-serv-vnic)#exit
ISR4331(config-virt-serv)#activate
% Activating virtual-service 'SNORT', this might take a few minutes. Use 'show virtual-service list' for progress.


ISR4331(config-virt-serv)#
*Mar  4 08:15:08.904: %ONEP_BASE-6-CONNECT: [Element]: ONEP session Application:utd_snort Host:ISR4331_RP_0 ID:9249 User: has
connected.% UTD: Received appnav notification from LXC for  (src 192.168.0.1, dst 192.168.0.2)


*Mar  4 08:15:11.272: %VIRT_SERVICE-5-ACTIVATION_STATE: Successfully activated virtual service SNORT
*Mar  4 08:15:12.303: %VMAN-5-VIRT_INST_NOTICE: SIP1: vman:  VIRTUAL SERVICE SNORT LOG: Mar  4 08:15:07 ISR4331_RP_0
Nodemgr: %CSRMGMT-NODEMGR-5-619072: Process with pid 66 exits
*Mar  4 08:15:13.229: %LINK-3-UPDOWN: Interface VirtualPortGroup0, changed state to up
*Mar  4 08:15:13.260: %LINK-3-UPDOWN: Interface VirtualPortGroup1, changed state to up
*Mar  4 08:15:14.229: %LINEPROTO-5-UPDOWN: Line protocol on Interface VirtualPortGroup0, changed state to up
*Mar  4 08:15:14.260: %LINEPROTO-5-UPDOWN: Line protocol on Interface VirtualPortGroup1, changed state to up
ISR4331(config-virt-serv)#
ISR4331(config-virt-serv)#
```

シグニチャー アップデート

- どこから？

cisco.com からの場合

設定例)

```
utd engine standard
  signature update server cisco username <CCO username> password <CCO password>
  signature update occur-at daily 0 0
```

Local Server からの場合

設定例)

```
utd engine standard
  signature update server url http://x.x.x.x/directoryname/filename
  signature update occur-at weekly 1,3,5 05 00
```

- いつ？

スケジュールアップデート

```
utd engine standard
  signature update server cisco username <CCO username> password <foo>
  signature update occur-at daily 0 0
```

マニュアルアップデート Execモードで下記コマンドを実行

```
Router# utd signature update server cisco username <CCO username> password <CCO password>
```

参考URL

- Snort IPS
  https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-3s/sec-data-utd-xe-3s-book/snort-ips.html#task_9ECA778E372F4E168184D16BB7BF0138
- Snort IPS Deployment Guide
  http://www.cisco.com/c/en/us/products/collateral/security/router-security/guide-c07-736629.html#_Toc442352489
- Cisco Snort IPS for the Cisco 4000 Series Integrated Services Routers FAQ
  http://www.cisco.com/c/en/us/products/collateral/security/router-security/q-and-a-c67-736113.html
- Cisco Snort IPS for 4000 Series Integrated Services Routers Data Sheet
  http://www.cisco.com/c/en/us/products/collateral/security/router-security/datasheet-c78-736114.html


CISCO
TOMORROW starts here.