

# SecIntel on MX 設定ガイド

Juniper Networks .K.K

2020年7月31日

JUNIPER  
NETWORKS

Engineering  
Simplicity

# 更新履歴

バージョン	更新日	更新内容
1.0	2020/7/31	初版公開

# はじめに

本資料にある内容は、資料作成時点におけるものであり、事前の予告なしに内容を変更する場合があります。

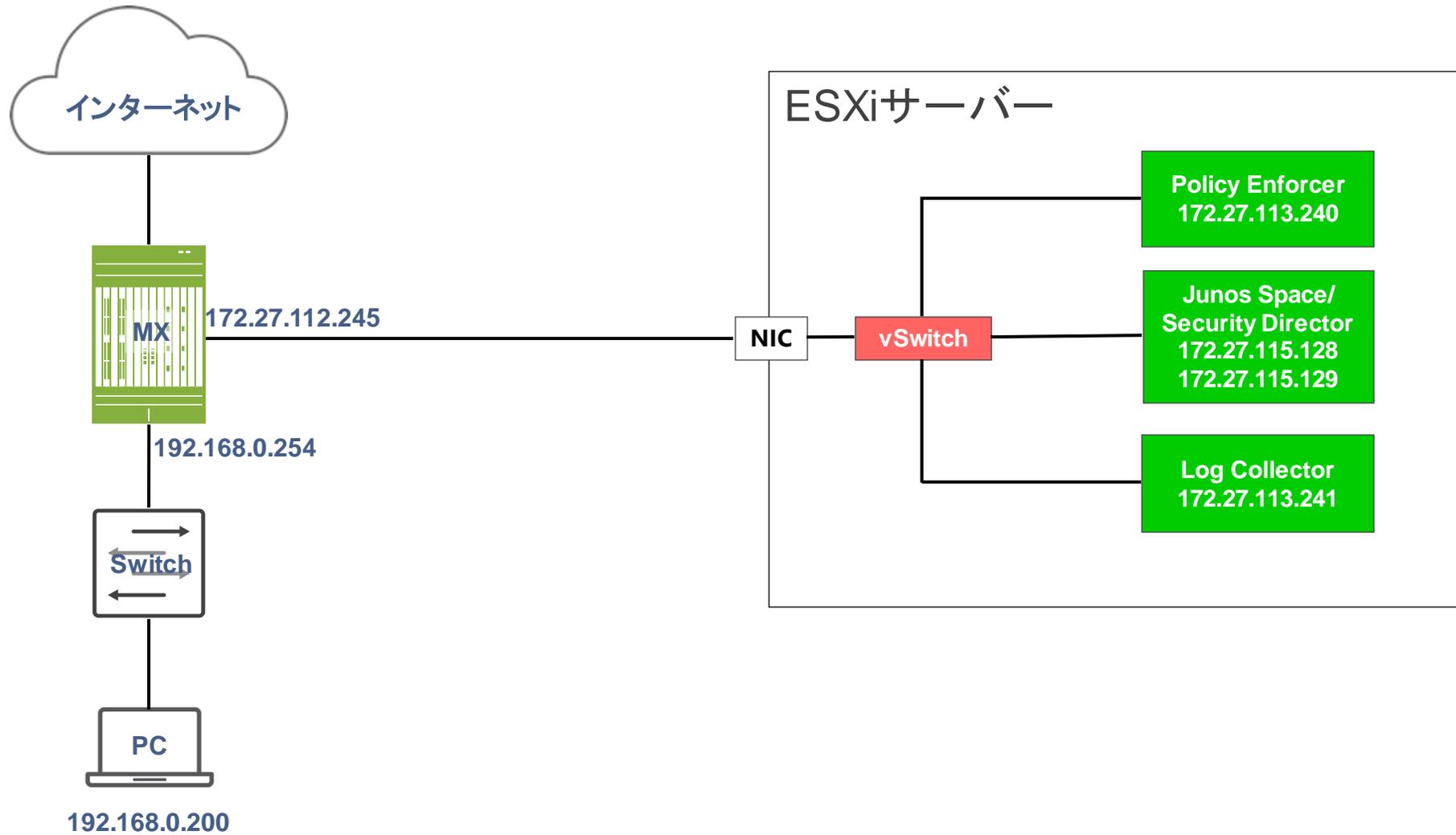
本資料は内容の正確さを保つために努めて作成しておりますが、本資料を利用することによって生じた損害について、当社は一切責任を負わないものとします。

また、本資料の内容と公式情報との間に差分がある場合、公式情報を正としてお取り扱いください。

本資料は下記のソフトウェア/サービスを用いてConnected Securityのセットアップを行っています。

- ESXi 6.0
- space-19.4R1.3.ova
- Security-Director-19.4R1.53.img
- Policy\_Enforcer-19.4R1-975.ova
- Log-Collector-19.4R1.28.ova
- MX240(OS Version 19.4R1.10)

# 構成イメージ



# Agenda

- 事前準備・設定
- Security Director設定
- MX設定
- MX確認コマンド一例



# 事前準備・設定



# 事前準備・設定

1. Junos Space、Log Collector、Policy Enforcerのデプロイ・各初期設定を行う
2. Junos SpaceにSecurity Directorをインストールする
3. Device Discovery ProfilesでMXを登録する  
(※MX側でIPアドレス・SNMPの事前設定が必要となります)
4. 登録したMXのOSバージョンに合わせたDMIスキーマをインストールする
5. Sky ATPアカウントを持っていない場合は下記ポータルサイトでアカウントを作成  
<https://sky.junipersecurity.net/>

-アカウント作成方法は下記URLを参照

[https://www.juniper.net/documentation/en\\_US/release-independent/sky-atp/topics/task/configuration/sky-atp-registering.html](https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/task/configuration/sky-atp-registering.html)

※本年から Sky ATPはATP Cloudへ名称を変更させて頂きました。

GUI上や各ドキュメント上の表記につきましては、ATP Cloud に随時変更させて頂く予定でございます。

本マニュアルは、変更前の現在のGUI上の表記に合わせてSky ATP の名称で作成しております。

# Security Director設定



# Security Director基本設定の流れ

1. Log Collectorの設定
2. Policy Enforcerの設定
3. Secure Fabricの設定
  - Secure Fabric : ネットワークデバイスの集合
4. Sky ATPの設定
  - アカウント作成済みのSky ATP/Realmの指定

# Log Collectorの設定

The screenshot shows the SPACE dashboard interface. In the left-hand navigation menu, 'Security Director' is highlighted with a red box. A callout box with a green border and a yellow arrow points to this menu item, containing the text 'Security Directorを選択' (Select Security Director). The main dashboard area displays several components:

- System Health Report:** A table listing various system health issues with their status and a 'Click' link for more details.
- Fabric Load History:** A line graph showing 'Average CPU usage' over the 'Past 1 minute'. The usage starts around 25, drops to 20, and then spikes to 50.
- Active Users History:** A line graph showing 'Active user count' over the 'Past 1 minute'. The count remains constant at approximately 1.0.
- Overall System Condition:** A semi-circular gauge with three segments: 'Good' (green, 0-30), 'Average' (yellow, 30-75), and 'Poor' (red, 75-100). The needle is positioned at approximately 45.

Process	Parameter	Status	More D...
Fabric	VIP Bind issue detected in JBoss node(s)	No	<a href="#">Click</a>
Fabric	Fabric node with down state is detected	No	<a href="#">Click</a>
Fabric	Audit Logs forwarding failed	No	<a href="#">Click</a>
Fabric	High CPU detected in last 3 days	No	<a href="#">Click</a>
Fabric	CPU counters are inactive	No	<a href="#">Click</a>
Fabric	Disk utilization is abnormal	No	<a href="#">Click</a>
MySQL	Tables exceed the size limit (>10 GB)	No	<a href="#">Click</a>
Fabric	Management sessions are mismatched with UI data	No	<a href="#">Click</a>
JBoss	HPROF availability	No	<a href="#">Click</a>
JBoss	JBoss restart observed in last 3 days	No	<a href="#">Click</a>
Fabric	Process are running incorrectly	No	<a href="#">Click</a>
JBoss	Multi-Master detected (App Logic)	N/A	<a href="#">Click</a>

# Log Collectorの設定

Administration / Logging Management / Logging Nodes

## Logging Nodes

①クリック

②クリック

③クリック

④クリック

Name	Node Type	Node IPv4	Node IPv6	Status	Application	Version	Last Boot Time
No data available							

# Log Collectorの設定

Add Logging Node ②

Progress: Select Deployment (Active) | Add Collector Node | Certificate Details

Log Collector type

- Security Director Log Collector ✓
- Security Director Log Collector**
- Juniper Secure Analytics

① Security Director Log Collector を選択

② クリック

Cancel Next

# Log Collectorの設定

Add Logging Node ?

Progress: Select Deployment (0%), Add Collector Node (100%), Certificate Details (0%)

### Add Collector Node

Node 1

Node Name* ?	<input type="text" value="LOG-COLLECTOR"/>
IP Address* ?	<input type="text" value="172.27.113.241"/>
User Name* ?	<input type="text" value="admin"/>
Password* ?	<input type="password" value="*****"/>

①各項目に入力する

②クリック

Buttons: Cancel, Back, Next

# Log Collectorの設定

## Add Logging Node ?

Progress: Select Deployment, Add Collector Node, **Certificate Details**

### Certificate Details

#### Issued To

Common Name (CN)	LOG-COLLECTOR
Organization (O)	Juniper Networks
Organization Unit (OU)	Juniper Networks
Serial Number	1

#### Issued By

Common Name (CN)	Juniper Networks
Organization (O)	Juniper Networks, Inc.
Organization Unit (OU)	Juniper Networks, Inc.

Buttons: Cancel, Back, **Finish**

Annotation: クリック (Click) pointing to the Finish button.

# Log Collectorの設定

## Add Logging Node ?

**Summary**  
Review the summary of configuration changes.

<b>Deployment Information</b>	<a href="#">Edit</a>
Log Collector type	Security Director Log Collector
<b>Add Collector Node Infor...</b>	<a href="#">Edit</a>
Node Name	LOG-COLLECTOR
IP Address	172.27.113.241
User Name	admin

Click OK to complete.

クリック

Cancel Back OK

# Log Collectorの設定

Administration / Logging Management / Logging Nodes

## Logging Nodes

	Node Name	Node Type	Node IPv4	Node IPv6	Status	Application	Version	Last Boot Time
<input type="checkbox"/>	LOG-COLLECTOR	Security Director L...	172.27.113.241	-	UP	GREEN	19.4R1.28	NA

1 items

確認

# Policy Enforcerの設定

The screenshot shows the 'Settings' page for the Policy Enforcer. The left sidebar contains a navigation menu with the following items: My Profile, Users & Roles, Logging Management, Monitor Settings, Signal, License Management, Policy Enforcer (highlighted with a red box), Settings (highlighted with a red box), Connectors, NSM Migration, and Policy Sync (highlighted with a red box). The main content area is titled 'Settings' and contains the following fields and options:

- IP Address\*: 172.27.113.234
- Username: root
- Password\*: [masked]
- Sky ATP Configuration Type: Sky ATP/JATP with Juniper Connected Security (selected)
- Poll Network wide endpoints\*: 24 hours
- Poll Site wide endpoints\*: 5 mins
- Buttons: OK, Reset

Numbered callouts in green boxes point to the following elements:

- ①クリック: Points to the 'Signal' menu item.
- ②クリック: Points to the 'Policy Sync' menu item.
- ③Policy EnforcerのIPアドレスを入力: Points to the IP Address input field.
- ④パスワードを入力: Points to the Password input field.
- ⑤Sky ATP/JATP with Juniper Connected Securityを選択: Points to the Sky ATP Configuration Type dropdown menu.
- ⑥クリック: Points to the 'OK' button.

# Policy Enforcerの設定

The screenshot shows the Juniper Policy Enforcer Settings page. The left sidebar contains navigation options: My Profile, Users & Roles, Logging Management, Monitor Settings, Signature Database, License Management, Policy Enforcer (expanded), NSM Migration, and Policy Sync Settings. The main content area is titled 'Settings' and includes a breadcrumb 'Administration / Policy Enforcer / Settings'. A search bar at the top right contains the text 'Global'. A blue information box at the top of the settings area states: 'Specify the Policy Enforcer virtual machine and login credentials to use for threat prevention.' The settings form includes fields for IP Address\* (172.27.113.234), Username?, Password\*, Sky ATP Configuration Ty..., Poll Network wide endpoi..., and Poll Site wide endpoints\* (5 mins). A modal dialog box titled 'Sky ATP/JATP Feed Connector' is overlaid on the form. The dialog contains a note: 'Note: Once the system is configured with Sky ATP with Policy Enforcer as its Threat Prevention Type, it will not be able to switch to Sky ATP or Cloud feeds only types.' The dialog has 'Cancel' and 'OK' buttons. A green callout box with the Japanese text 'クリック' (Click) points to the 'OK' button in the dialog.

# Policy Enforcerの設定

The screenshot shows the Juniper Policy Enforcer Settings page. The left sidebar contains navigation options: My Profile, Users & Roles, Logging Management, Monitor Settings, Signature Database, License Management, Policy Enforcer (selected), Connectors, NSM Migration, and Policy Sync Settings. The main content area is titled 'Settings' and includes a breadcrumb 'Administration / Policy Enforcer / Settings'. A search bar at the top right contains the text 'Global'. A modal dialog box titled 'Sky ATP/JATP Feed Connector' is displayed in the center. The dialog text reads: 'Policy Enforcer is now successfully configured. Would you like to setup your Threat Policies in Guided Setup?'. At the bottom of the dialog are 'Cancel' and 'OK' buttons. A red box highlights the 'Cancel' button, and a green callout bubble with the text 'クリック' (Click) points to it. Another green callout bubble at the top of the dialog contains the text: '※OKをクリックするとGuided Setupに進みますが今回は使用しないためCancelを選択します' (Note: Clicking OK will proceed to Guided Setup, but since we are not using it this time, we will select Cancel).

# Policy Enforcerの設定

Administration / Policy Enforcer / Settings

Settings ?

**i** The Policy Enforcer Space API user (pe\_user) password is currently valid. It will expire on 2020-10-06.

**✓** The Policy Enforcer is active.  
It is configured with version 19.4R1-975.

**重要 : Activeになったのを確認**

IP Address\* 172.27.113.234

Username ? root

Password\*

Sky ATP Configuration Ty... ? Sky ATP/JATP with Juniper Connected Security ▾

Configure polling timers to discover hosts in your network

Poll Network wide endpoi... \* ? 24 hours

Poll Site wide endpoints\* ? 5 mins

OK Reset

Policy Enforcer Logs Download

# Secure fabricの設定

The screenshot displays the Juniper SD-WAN management interface. The left-hand navigation menu is highlighted with a red box, and the 'Secure Fabric' option is selected. The main content area shows the 'Secure Fabric' configuration page, which includes a search bar, a table for 'Sites', and an 'Add Enforcement Points' button. Three callout boxes with green borders and arrows point to specific elements: '①クリック' points to the menu icon, '②クリック' points to the 'Secure Fabric' menu item, and '③クリック' points to the '+' icon in the 'Add Enforcement Points' button.

Devices / Secure Fabric

Global

## Secure Fabric ?

Sites

Add Enforcement Points +

Site	Enforcement P...	IP	Model	Feed Source	Feed So...	Last Up...	Desc...
No data available							

# Secure fabricの設定

Create Site ?

① サイト名を入力

Site\* Test-Site

Description Write description..

② クリック

Cancel OK

# Secure fabricの設定

Devices / Secure Fabric

Global

## Secure Fabric

Sites

Add Enforcement Points + ✎ 🗑

<input type="checkbox"/>	Site	Enforcement P...	IP	Model	Feed Source	Feed So...	Last Up...	Desc...
<input type="checkbox"/>	Test-Site	Add Enforceme...	—	—	—	—	—	—

1 items ↻

①クリック

# Secure fabricの設定

Add Enforcement Points ?

**i** Assigning a device to the site will cause a change in the device configuration.

Specify the enforcement points to assign to the site. The site cannot contain both switches and connectors.

Enforcement Points

0 Available

<input type="checkbox"/>	Name	IP	Model
No available items			

1 Selected

<input type="checkbox"/>	Name	IP	Model
<input type="checkbox"/>	BIG-ZAM	172.27.112.245	MX240

①対象のMXを右側のウィンドウへ移動

Perimeter Device ?

× BIG-ZAM

②クリック

Cancel OK

# Secure fabricの設定

The screenshot displays the 'Secure Fabric' configuration page in a management console. The left sidebar contains navigation options: Security Devices, Device Discovery, Secure Fabric (selected), NSX Managers, and vCenter Servers. The main content area shows a 'Secure Fabric' header and a 'Sites' table. The table has columns for Site, Enforcement P..., IP, Model, Feed Source, Feed So..., Last Up..., and Desc... A single row is visible, highlighted with a red border, representing a site named 'Test-Site' with enforcement points 'BIG-ZAM' and IP address '172.27.112.245'. A green callout box with a pointer to the 'BIG-ZAM' enforcement point contains the Japanese text 'サイトにデバイスが登録されたのを確認'.

Site	Enforcement P...	IP	Model	Feed Source	Feed So...	Last Up...	Desc...
Test-Site	BIG-ZAM	172.27.112.245	MX240	—		July 29, 2...	—

# Sky ATPの設定

Configure / Threat Prevention / Feed Sources

Global

Feed Sources

Sky ATP JATP Custom Feeds

①クリック

②クリック

③クリック

④クリック

Realm	Sites	Devices	Location	Enrollment Status	Token Expiry	Feed Status
0 items						

# Sky ATPの設定

Add Sky ATP Realm ?

Progress: SkyATP Realm Credential (Active) | Site | Global Configuration

### Sky ATP realm credentials

Provide your Sky ATP realm credentials

Location\*

Username

Password

Realm ?

No Sky ATP account? Select your region using the Location in the menu above, then [click here](#) to create an account. You will be redirected to the Sky ATP account page.

[Cancel](#) [Next](#)

①Sky ATPのアカウント/Realmを入力

※Sky ATPのアカウント作成がまだの場合はここからSky ATPポータルに移動可能

②クリック

# Sky ATPの設定

Add Sky ATP Realm ?

Progress: Sky ATP Realm Credential | **Site** | Global Configuration

**Info**  
Assigning a site to the realm will cause a change in the device configuration in the associated devices.

**Site**  
Realm: new-shirata

Choose sites to be enrolled into the realm.

Site:  × Test-Site ▼ [Create new site](#)

① Sky ATPのRealmにサイトを登録する

② クリック

Cancel Next

# Sky ATPの設定

Add Sky ATP Realm ?

SkyATP Realm Credential Site **Global Configuration**

**Additional Settings**

IPv6 Feeds ?

**Infected Hosts**  
Select a threshold level to block infected hosts.

Threat Level Threshold

1 2 3 4 5 6 7 8 9 10

閾値を設定

Administrators Who Receive Email Notifications + ✎ 🗑

Cancel Finish



# Sky ATPの設定

The screenshot displays the Juniper Sky ATP configuration page for 'Feed Sources'. The left sidebar shows the navigation menu with 'Threat Prevention' expanded to 'Feed Sources'. The main content area shows the 'Feed Sources' configuration page with tabs for 'Sky ATP', 'JATP', and 'Custom Feeds'. A table lists the configured feed sources, with one entry highlighted by a red box. A green callout box points to the 'Feed Status' column of this entry, containing the text '登録できたことを確認' (Confirm that registration was successful).

<input type="checkbox"/>	Realm	Sites	Devices	Location	Enrollment Status	Token Expiry	Feed Status	Last Downloaded
<input type="checkbox"/>	new-shirata	Test-Site	BIG-ZAM	North America	SUCCESS	Jul 29, 2021	✔ OK	Jul 29, 2020, 11:3...

1 items

登録できたことを確認

# MX設定



# MX設定

## 1. MXがNetConfを受け入れるようにする

```
system {  
  services {  
    netconf {  
      ssh {  
        port 830;  
      }  
    }  
  }  
}
```

# MX設定

## 2. SecIntelの設定

```
services {
  security-intelligence {
    url https://172.27.113.234:443/api/v1/manifest.xml; #Security Directorと連携時に自動入力
    authentication {
      auth-token 6XYNM4KKLPSI16FOC1LYKIDOD2K9GYK0; #Security Directorと連携時に自動入力
    }
    traceoptions {
      file secIntel.log size 1g;
      level all;
      flag feed;
    }
  }
}
```

# MX設定

## 3. URL Filteringの設定

```
services {
  web-filter {
    profile Profile_Name { #任意のプロファイル名
      security-intelligence-policy {
        file-type txt; #txtのみサポート
        threat-level 1 { #threat-levelは1~10の各レベルごとに設定
          threat-action {
            accept; #アクションを指定*1
          }
        }
      }
    }
  }
}
```

\*1 threat-actionはlog、drop、drop-log、accept、log-and-sample、drop-and-sample、drop-log-and-sampleから選択

# MX設定

## 4. URL Filter Templateの設定

```
services {
  web-filter {
    profile Profile_Name {
      url-filter-template Template_Name { #任意のテンプレート名
        client-interfaces xe-2/0/0.0; #URLフィルターを適応するインターフェイスを指定
        client-routing-instance inet.0;
      }
    }
  }
}
```

# MX確認コマンド一例



# MX確認コマンド一例

- Security-Intelligenceの概要の確認

```
> show services security-intelligence category summary
```

```
Category name      :CC  
Status             :Enable  
Description        :Command and Control data schema  
Update interval   :1800s  
TTL                :3456000s  
Feed name         :cc_ip_data  
Version           :20200723.4  
Objects number    :144238  
Create time       :2020-07-29 12:44:12 JST  
Update time       :2020-07-29 13:06:49 JST  
Update status     :Store succeeded  
Expired           :No  
Options           :N/A
```

# MX確認コマンド一例

- Security-Intelligenceの更新ステータスの確認

```
> show services security-intelligence update status
```

```
Current action      :Checking update interval of category CC.  
Last update status  :Update interval of category CC is not reached.  
Last connection status:succeeded  
Last update time    :2020-07-29 13:22:04 JST
```

# MX確認コマンド一例

- Policy Enforcerから受信した脅威レベルごとのフィルター数及びフィルターの保存場所の確認

```
> show services web-filter secintel-policy-status summary profile Profile_Name
```

```
URL Filtering SecIntel Policy Status:
```

```
Profile      : Profile_Name
```

```
C&C DB File  : /var/db/url-filterd/urlf_si_cc_db.txt*1
```

```
Policy State: Ready
```

```
DB File Change Time : Wed Jul 29 12:28:18 2020
```

```
DB File Load Time   : Wed Jul 29 12:28:19 2020
```

```
C&C Prefix Count    : IPv4: 144238      IPv6: 0
```

```
Filters:
```

Threat level	Action	v4 Term Count	IPv4	v6 Term Count	IPv6
1	ACCEPT	192	57595	0	0
2	ACCEPT	26	7597	0	0
3	ACCEPT	4	1044	0	0
4	ACCEPT	4	1082	0	0
5	ACCEPT	5	1254	0	0
6	ACCEPT	170	50913	0	0
7	ACCEPT	5	1370	0	0
8	ACCEPT	5	1498	0	0
9	ACCEPT	4	971	0	0
10	ACCEPT	4	1119	0	0

\*1 Secure Fabric上でSky ATPにサイトを登録すると、Sky ATPからC&C DBファイルをPolicy EnforcerへプッシュされMXがそれを取得する



# Thank you

---

JUNIPER  
NETWORKS®

Engineering  
Simplicity