Encrypted Traffic Insights 設定ガイド

Juniper Networks .K.K

2020年9月10日

Juniper Networks | Engineering Simplicity

更新履歴

バージョン	更新日	更新内容
1.0	2020/9/10	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ETI(※1)のセットアップを行っています。

- SRX1500 (OS Version 20.2R1)
- Sky ATP (※2)

※1 **ETA(Encrypted Traffic Analyze)**は**ETI(Encrypted Traffic Insights)**に名称を変更させて頂きました。

※2 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。

Encrypted Traffic Insight(ETI)とは？

ETI機能は、SSL通信を制御する為に必要な機能です。

ETI機能を使用して、暗号化されるまでの証明書のやり取りやSNIの情報、SSL通信の振舞をSky ATPへ集約します。

Sky ATP内で動作する機械学習エンジンがETI機能で集約した情報を蓄積し、SecIntel(脅威インテリジェンス)機能を利用して不正な証明書情報や通信の振舞分析により、悪意のあるサイトとのSSL通信をブロックし、アラートログの出力をします。

尚、ETI機能単独ではSSL通信の暗号化に不正がある場合(Alert)は、その通信をブロックします。

ETIの動作について

暗号化された脅威を検出するための2つの新しいメカニズムを導入します:
-悪意のある既知の証明書リストのフィード
-クラウドでの機械学習エンジンによる検出

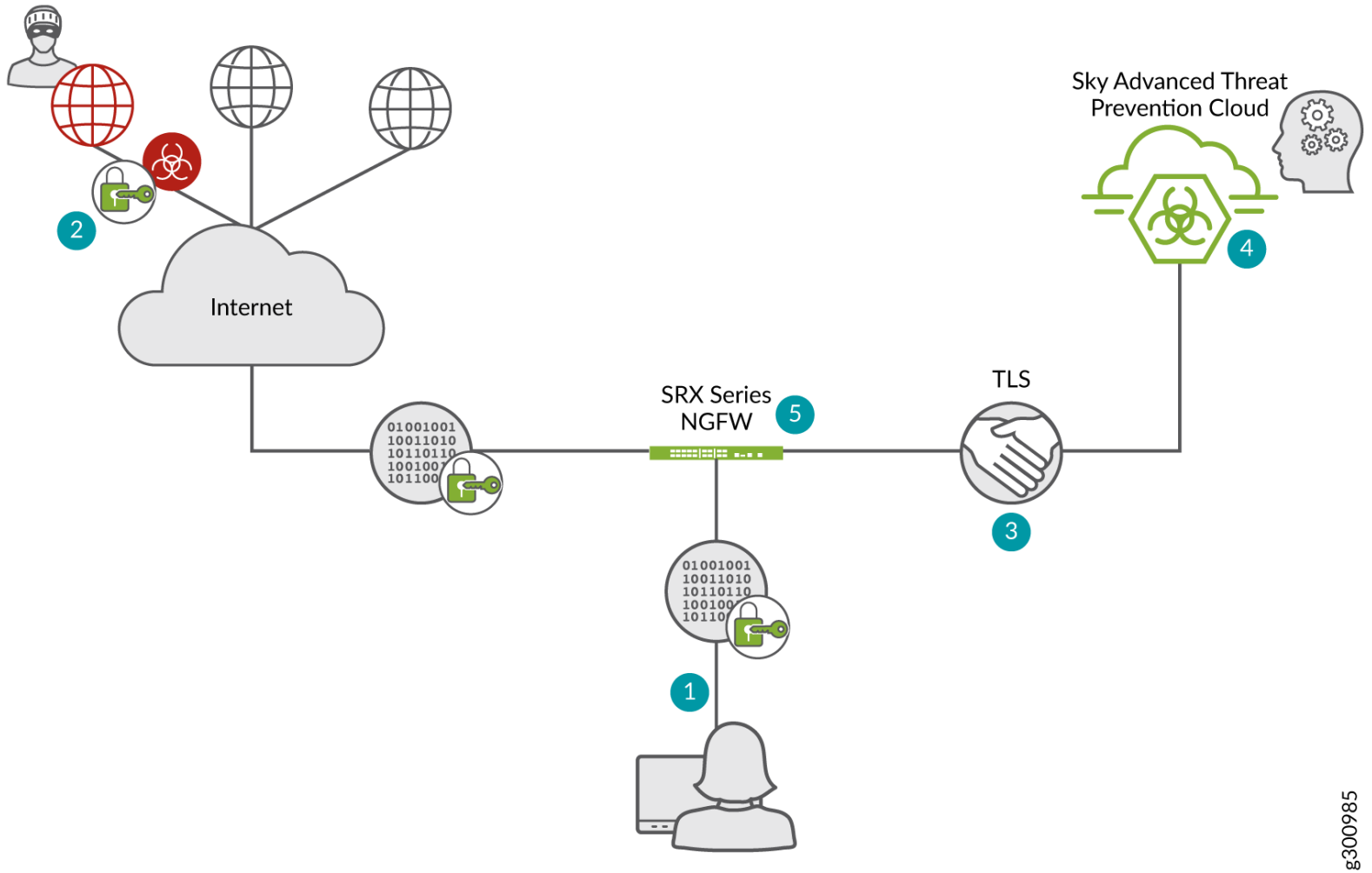
1. クライアントはインターネットへの暗号化されたコネクションを作成します。

2. Sky ATPからSRXにフィードされた悪意のある既知の証明書リストを用いて、検知を試みます。

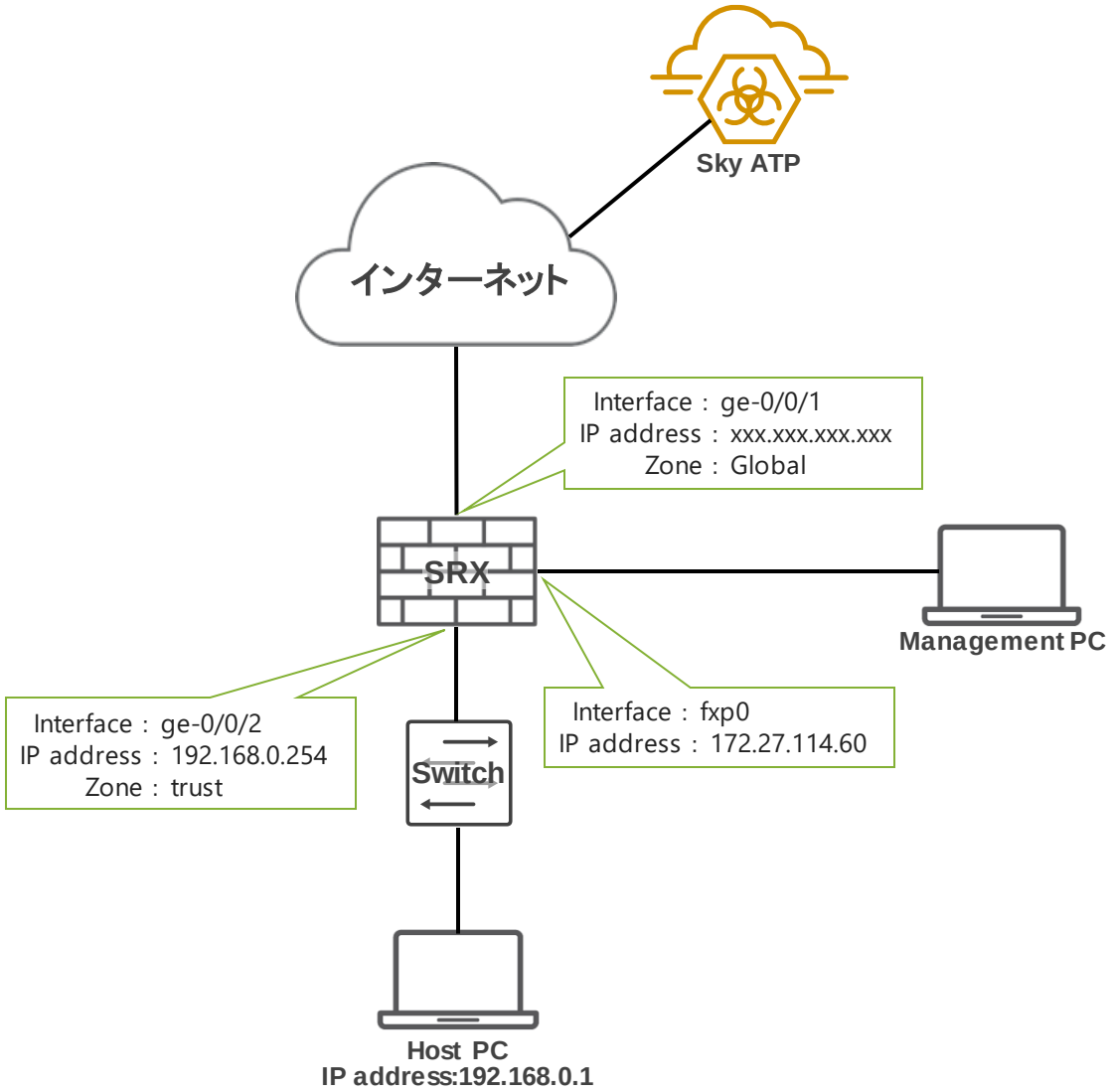
3. SRXはコネクションのメタデータをSky ATPに送信します。

4.機械学習エンジンはこれが悪意のあるコネクションであるかどうかを判断します。

5.悪意のあるコネクションであるとSky ATPが判断した場合は、SRXに検知結果をフィードし、該当通信をブロックします。



構成イメージ



Agenda

- 事前準備・設定
- SRX設定
- ATP Cloud設定
- 確認コマンド一例
- 注意事項
- Appendix

事前準備・設定

事前準備・設定

1. SRXのIPアドレス・Zone・Policy含む基本設定を行う
   ※Junos OS v20.2以降必須

2. 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

   ※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。

SRX設定

SRX設定について

- システム関連・IPアドレス・ゾーン・ポリシーなどの基本設定は事前に行ってください
- ETIの設定を行う
  -次ページ以降を参照
- SecIntelの設定を行う
  -P.14以降を参照

ETI設定

1. セキュリティメタデータストリーミングポリシーを作成する

```
services {
    security-metadata-streaming {
        policy [security-metadata-streaming-policy-name] {
            http {
                action permit;
                notification {
                    log;
                }
            }
        }
    }
}
```

入力例：

```
set services security-metadata-streaming policy ETI_Policy http action permit
Set services security-metadata-streaming policy ETI_Policy http notification log
```

ETI設定

2. セキュリティメタデータストリーミングポリシーをファイアウォールポリシーにアタッチする

```
security {
    policies {
        from-zone [from-zone-name] to-zone [to-zone-name] {
            application-services {
                security-metadata-streaming-policy [security-metadata-streaming-policy-name];
            }
        }
    }
}
```

入力例：

```
set security policies from-zone trust to-zone Global application-services security-metadata-
streaming-policy ETI_Policy
```

SecIntel設定

1. SecIntelプロファイルを作成する

```
services {
    security-intelligence {
        profile [profile-name] {
            category [secintel-category-name];
        }
    }
}
```

入力例：

```
set services security-intelligence profile Secintel-profile category CC
```

SecIntel設定

2. SecIntelプロファイルルールを作成、検知時の動作を設定する

```
services {
    security-intelligence {
        profile [profile-name] {
            rule [profile-rule-name] {
                match {
                    threat-level [threat-level]; #Threat levelは1〜10から選択、複数選択時は[8 9 10]のように入力
                }
                then {
                    action {
                        [permit/block close/block drop/recommended];
                    }
                    log;
                }
            }
        }
    }
}
```

SecIntel設定

入力例：

```
set services security-intelligence profile Secintel-profile rule CC_rule-1 match threat-level [1 2
3 4 5 6 7]
set services security-intelligence profile Secintel-profile rule CC_rule-1 then log
set services security-intelligence profile Secintel-profile rule CC_rule-1 then action permit
set services security-intelligence profile Secintel-profile rule CC_rule-2 match threat-level [8 9
10]
set services security-intelligence profile Secintel-profile rule CC_rule-2 then log
set services security-intelligence profile Secintel-profile rule CC_rule-2 then action block drop
```

SecIntel設定

3. SecIntelポリシーを作成し、SecIntelプロファイルをアタッチする

```
services {
    security-intelligence {
        policy [secintel-policy-name] {
            [secintel-category-name] {
                [profile-name];
            }
        }
    }
}
```

入力例：

```
set services security-intelligence policy Secintel-policy CC Secintel-profile
```

SecIntel設定

4. ファイアウォールポリシーにSecIntelポリシーをアタッチする

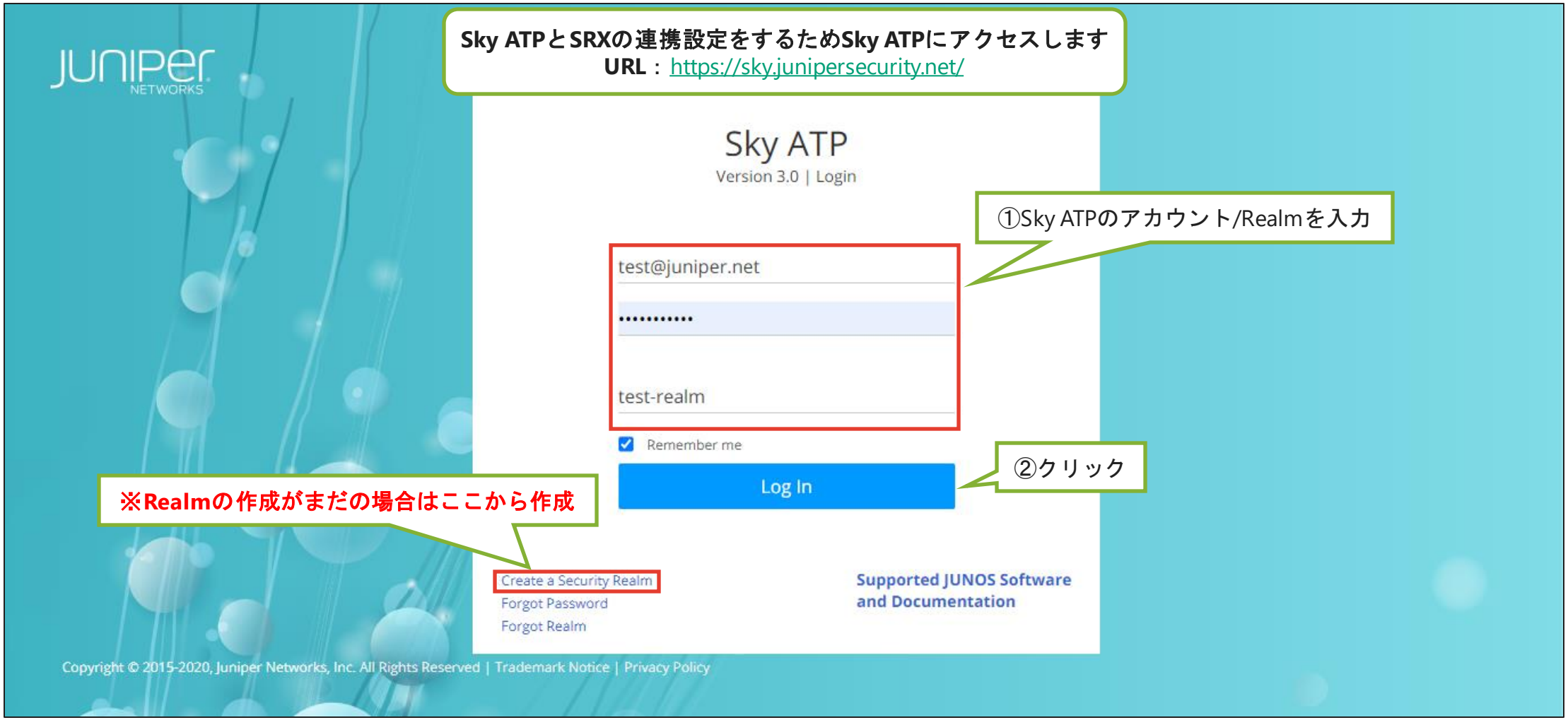
```
security {
    policies {
        from-zone [from-zone-name] to-zone [to-zone-name] {
            policy [security-policy-name] {
                match {
                    source-address local;
                    destination-address any;
                    application any;
                }
                then {
                    permit {
                        application-services {
                            security-intelligence-policy [secintel-policy-name];
                        }
                    }
                }
            }
        }
    }
}
```

入力例：

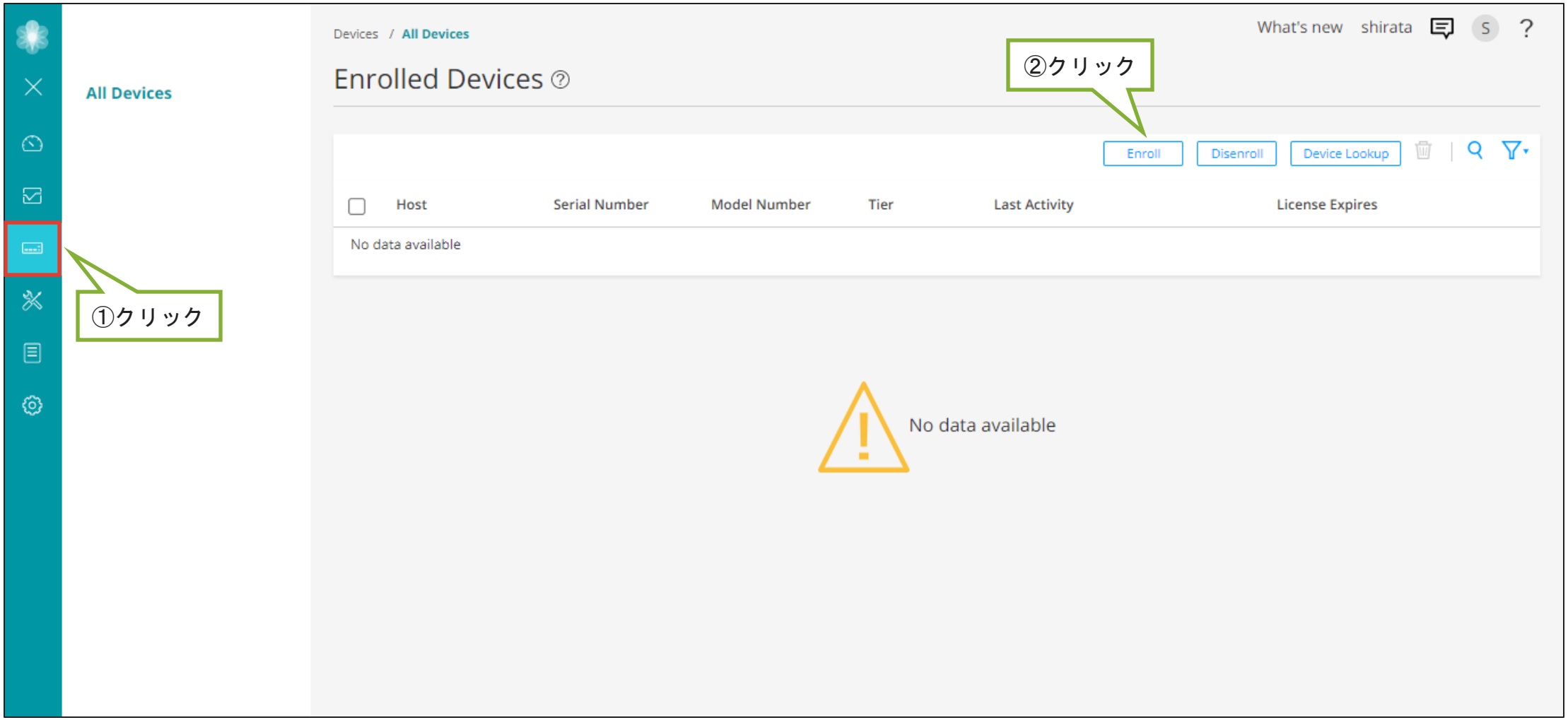
```
set security policies from-zone trust to-zone Global policy trust-to-Global then permit application-
services security-intelligence-policy Secintel-policy
```

Sky ATP設定

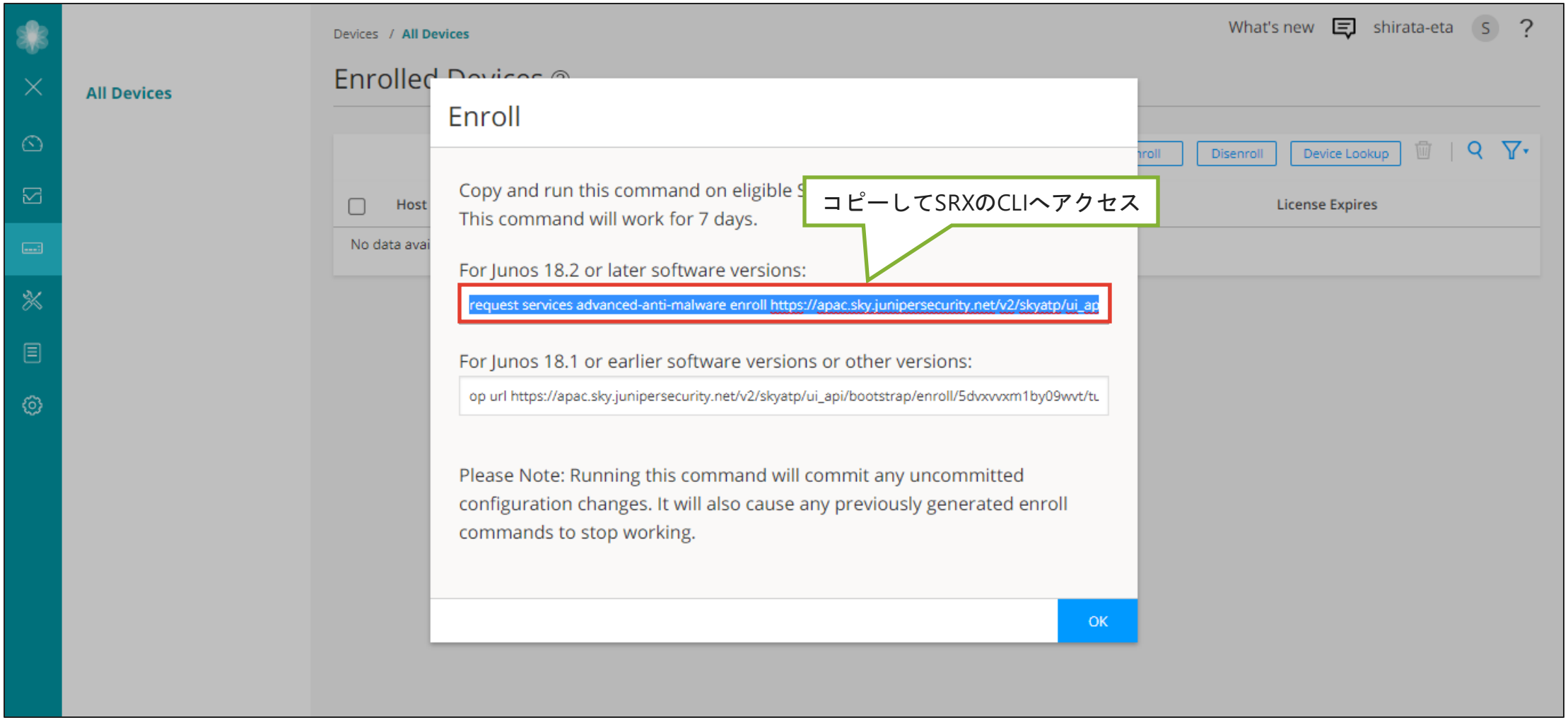
Sky ATP設定



Sky ATP設定



Sky ATP設定

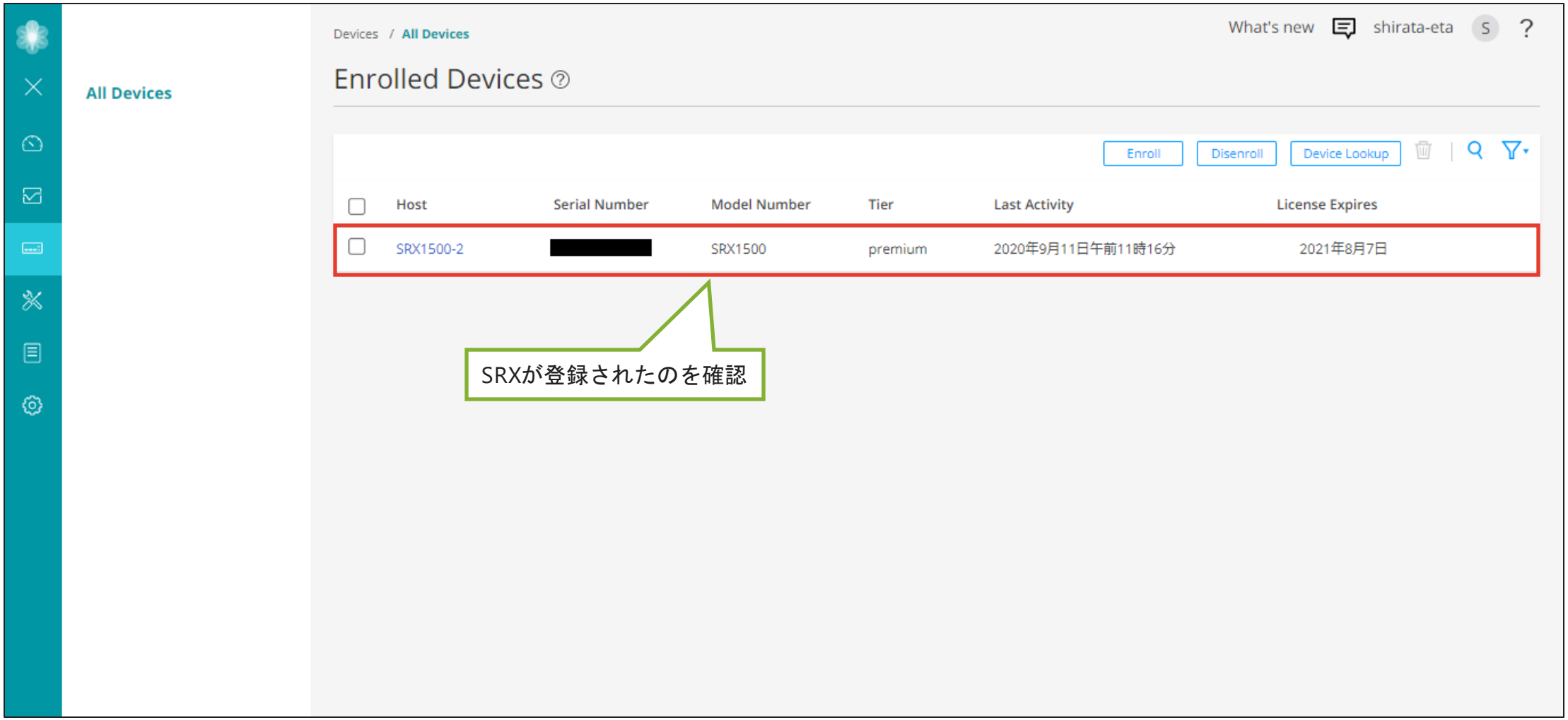


Sky ATP設定

先ほどコピーしたエンロールコマンドをSRXのCLIでペーストして実行

```
> request services advanced-anti-malware enroll
https://apac.sky.junipersecurity.net/v2/skyatp/ui_api/bootstrap/enroll/xxxxxxxxxxxxxxx/xxxxxxxxxxxxxxx.slax

Platform is supported by Sky ATP: SRX1500.
Version 20.2R1.10 is valid for bootstrapping.
Going to enroll single device for SRX1500: DBxxxxxxxxxx with hostname SRX1500-2.

~~~~~~~~~~~~~~~~~~~中略~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Configure security-intelligence service...
Configuration added successfully for security-intelligence service.
Check configuration on device...
SSL profile:                          [OK]
SecIntel CA:                          [OK]
Cloud CA:                             [OK]
Client cert found:                    [OK]
SSL profile action:                   [OK]
URL for advanced-anti-malware:        [OK]
Profile for advanced-anti-malware:    [OK]
URL for security-intelligence:        [OK]
Profile for security-intelligence:    [OK]
All configurations are correct for enrollment.
Communicate with cloud...
Wait for aamw connection status...
Device enrolled successfully!
```

Sky ATP設定



確認コマンド一例

確認コマンド一例

Sky ATPとの接続性の確認

```
> show services advanced-anti-malware status
Server connection status:
  Server hostname: srxapi.ap-northeast-1.sky.junipersecurity.net #Sky ATPの接続先クラウドによって変わります*1
  Server realm: test-realm
  Server port: 443
  Proxy hostname: None
  Proxy port: None
    Control Plane:
      Connection time: 2020-10-05 08:18:35 JST
      Connection status: Connected
    Service Plane:
      fpc0
        Connection active number: 16
        Connection retry statistics: 4261
```

*1 クラウド別URL一覧

APAC:
srxapi.ap-northeast-1.sky.junipersecurity.net

US:
srxapi.us-west-2.sky.junipersecurity.net

EU:
srxapi.eu-west-1.sky.junipersecurity.net

Canada:
srxapi.ca-central-1.sky.junipersecurity.net

確認コマンド一例

Sky ATPとの接続性の詳細確認

```
> request services advanced-anti-malware diagnostics srxapi.ap-northeast-1.sky.junipersecurity.net*1 detail
*1 Sky ATPの接続先クラウドによってURLは変わります(前ページ参照)

    [INFO]    Try to get IP address for hostname srxapi.ap-northeast-1.sky.junipersecurity.net
DNS check                                          : [OK]
    [INFO]    Try to test Juniper ATP server connectivity
    [INFO]    Successfully connected to srxapi.ap-northeast-1.sky.junipersecurity.net:443
    [INFO]    Successfully connected to ca.junipersecurity.net:8080
    [INFO]    Successfully connected to va.junipersecurity.net:80
Juniper ATP reachability check                     : [OK]
    [INFO]    Time difference between ATP server and this device: 0 second(s)
Time check                                         : [OK]
    [INFO]    Configuration checking passed: PKI
    [INFO]    Configuration checking passed: SSL
    [INFO]    Configuration checking passed: AAMW Connection
    [INFO]    Configuration checking passed: SecIntel URL
    [INFO]    Configuration checking passed: SecIntel Authentication
Configuration activation check                     : [OK]
    [INFO]    Try ICMP service in Juniper ATP
Juniper ATP ICMP service check                     : [OK]
    [INFO]    To-ATP connection is using ge-0/0/1.0, according to route
Interface configuration check                      : [OK]
Outgoing interface MTU is default value
    [INFO]    Check IP MTU with length 1472
IP Path MTU is 1472
SSL configuration consistent check                 : [OK]
```

確認コマンド一例

セキュリティメタデータストリーミングに関する統計の確認

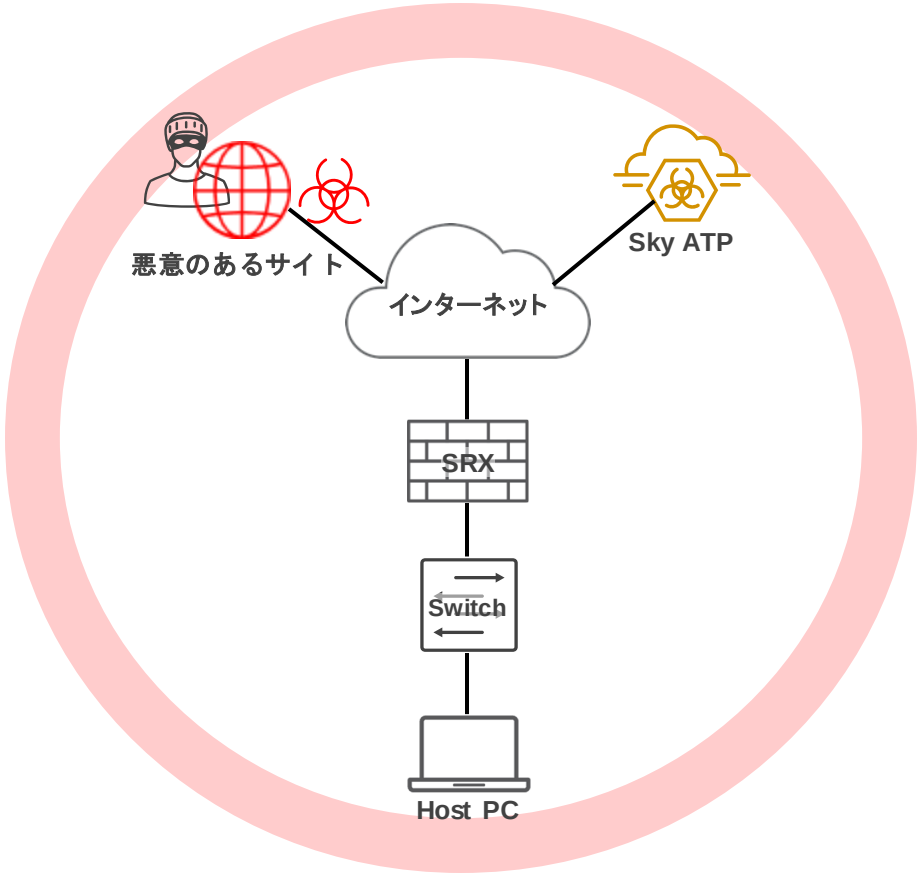
```
> show services security-metadata-streaming statistics

Security Metadata Streaming session statistics:  #セキュリティメタデータストリーミングセッションの統計
  Session inspected:    252  #検査されたセッションの数
  Session whitelisted:  0  #暗号化されたトラフィック分析のためにホワイトリストに登録されたセッションの数
  Session detected:     0  #悪意のある可能性があると検出されたセッションの数

Security Metadata Streaming submission statistics:  #セキュリティメタデータストリーミングの送信統計
  Records submission success:  141  #Sky ATPに正常に送信されたレコードの数
  Records submission failure:  0  #Sky ATPへ送信中に失敗したレコードの数
```

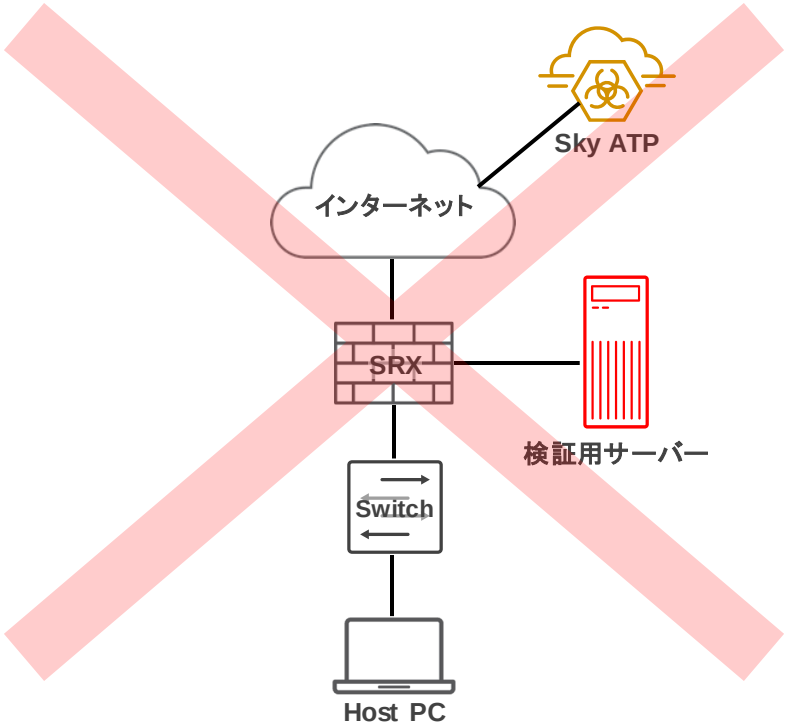
注意事項

注意事項

ETIは、Sky ATPがSRXから送られてくるメタデータを収集し、機械学習エンジンによりSecIntel機能を利用して悪意のあるサイト**(Global IP)**をブロックする機能となるため、**Private IP**を使用したローカルネットワーク上にある検証用のサーバーは検知対象外となります。

※ETI機能の詳細、動作についてはP.4、P.5を参照





Appendix

Appendix

本マニュアルに関するコンフィグを抜粋

```
# show
services {
    application-identification;
    ssl {
        initiation {
            profile aamw-ssl {
                trusted-ca [ aamw-secintel-ca aamw-cloud-ca ];
                client-certificate aamw-srx-cert;
                actions {
                    crl {
                        disable;
                    }
                }
            }
        }
    }
    advanced-anti-malware {
        connection {
            url https://srxapi.ap-northeast-1.sky.junipersecurity.net;
            authentication {
                tls-profile aamw-ssl;
            }
        }
    }
```

※Enrollコマンドにより自動入力

※Enrollコマンドにより自動入力

Appendix

```
security-metadata-streaming {
    policy ETA_Policy {
        http {
            action permit;
            notification {
                log;
            }
        }
    }
}
security-intelligence {
    url https://cloudfeeds-tokyo.sky.junipersecurity.net/api/manifest.xml;
    authentication {
        tls-profile aamw-ssl;
    }
    profile Secintel-profile {
        category CC;
        rule CC_rule-1 {
            match {
                threat-level [ 1 2 3 4 5 6 7 ];
            }
            then {
                action {
                    permit;
                }
```

※Enrollコマンドにより自動入力

Appendix

```
                    log;
                }
            }
            rule CC_rule-2 {
                match {
                    threat-level [ 8 9 10 ];
                }
                then {
                    action {
                        block {
                            drop;
                        }
                    }
                    log;
                }
            }
        }
        policy Secintel-policy {
            CC {
                Secintel-profile;
            }
        }
    }
}
```

Appendix

```
security {
    pki {
        ca-profile aamw-ca {
            ca-identity deviceCA;
            enrollment {
                url http://ca.junipersecurity.net:8080/ejbca/publicweb/apply/scep/SRX/pkiclient.exe;
            }
            revocation-check {
                disable;
                crl {
                    url http://va.junipersecurity.net/ca/deviceCA.crl;
                }
            }
        }
        ca-profile aamw-secintel-ca {
            ca-identity JUNIPER;
            revocation-check {
                crl {
                    url http://va.junipersecurity.net/ca/current.crl;
                }
            }
        }
        ca-profile aamw-cloud-ca {
            ca-identity JUNIPER_CLOUD;
            revocation-check {
```

※Enrollコマンドにより自動入力

Appendix

```
                crl {
                    url http://va.junipersecurity.net/ca/cloudCA.crl;
                }
            }
        }
    }
    policies {
        from-zone trust to-zone Global {
            policy trust-to-Global {
                match {
                    source-address local;
                    destination-address any;
                    application any;
                }
                then {
                    permit {
                        application-services {
                            security-intelligence-policy Secintel-policy;
                        }
                    }
                }
            }
            application-services {
                security-metadata-streaming-policy ETA_Policy;
            }
```

※Enrollコマンドにより自動入力

Appendix

```
        }
        from-zone Global to-zone trust {
            policy Global-to-trust {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    deny;
                }
            }
        }

    }
    zones {
        security-zone Global {
            interfaces {
                ge-0/0/1.0;
            }
            application-tracking;
        }
        security-zone trust {
            host-inbound-traffic {
                system-services {
```

Appendix

```
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                ge-0/0/2.0;
            }
            application-tracking;
        }
    }
}
interfaces {
    ge-0/0/1 {
        description Global;
        unit 0 {
            family inet {
                address xxx.xxx.xxx.xxx/28;
            }
        }
    }
    ge-0/0/2 {
        description Local-Network_For_ETA;
        unit 0 {
```

Appendix

```
            family inet {
                address 192.168.0.254/24;
            }
        }
    }
    fxp0 {
        description Management;
        unit 0 {
            family inet {
                address 172.27.114.60/22;
            }
        }
    }
}
```

SAMPLEコンフィグ

ETI_config.txt


Thank you
JUNIPER NETWORKS
Engineering
Simplicity