Cisco Firepower Next-Generation Firewall 6.3 Features Lab v1.2のご紹介

2019年4月18日

シスコシステムズ合同会社　セキュリティ事業
稲澤　敏

本日のアジェンダ

- Cisco Firepower Next-Generation Firewall概要
- 最新バージョン(Firepower 6.3)での新機能概要
- dCloud Lab利用方法
- Cisco Firepower Next-Generation Firewall 6.3 Features Lab v1.2シナリオ概要

Cisco Firepower
Next-Generation Firewall概要

Firepower シリーズが提供する脅威対策

次世代 Firewall

- ✓ アプリケーション制御
- ✓ ユーザ制御
- ✓ URL フィルタ
- ✓ Geo Location フィルタ

最も使われている IPS エンジン

- ✓ オープンソース IPS エンジン

運用の自動化 &イベント解析

- ✓ 自動チューニング、インパクト解析、インシデント相関分析
- ✓ 端末隔離機能 (CiscoISE 連携)

ネットワークとホストの可視化

- ✓ ネットワークとホスト学習

脅威情報フィルター

- ✓ Cisco 提供脅威情報活用
- ✓ 3rd パーティとの脅威情報連携

高度なマルウェア防御

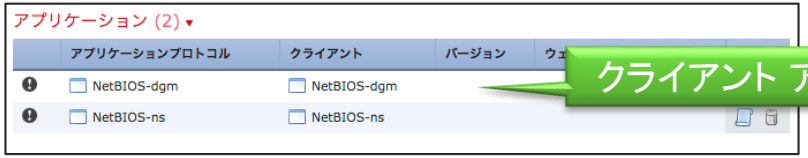
- ✓ シグネチャレスマルウェア検知
- ✓ マルウェアトラッキング
- ✓ クラウドリコール
- ✓ スレッドグリッドサンドボックス

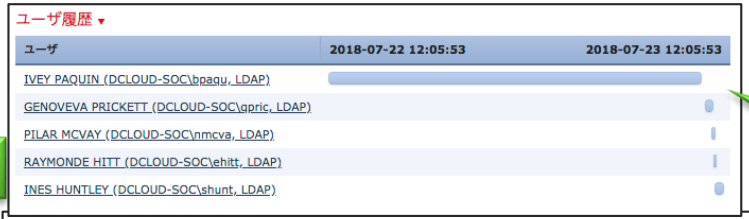
ネットワークマップ

- 対象ネットワーク上のホストに関する情報を収集し管理
- インシデント解析や自動チューニングのベースとなる情報
- 収集情報例
  - 存在するホスト (IPv4, IPv6)
  - ホップ数
  - オペレーティングシステム
  - アプリケーション
  - ポート
  - プロトコル
  - 脆弱性

インシデント解析例

例)アラートが発生したホストの情報を確認したい





侵入の痕跡

端末 OS

サーバ アプリケーション

クライアント アプリケーション

ユーザ履歴

該当脆弱性リスト

✓ 端末のセキュリティに関連する様々な情報を自動収集し、解析に活用

自動チューニングとインパクト解析

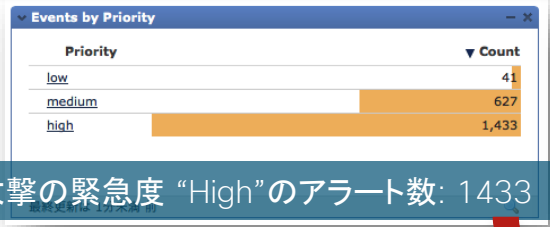
一般的な侵入検知機器 (IPS) の
運用者が抱える問題

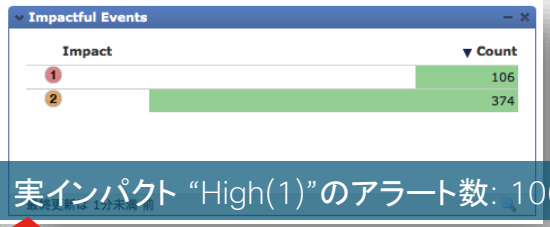
環境に合わせて設定を調整
したいが、運用が大変・・・

沢山のログが出るが、本当に
重要なものがわからない・・・

自動チューニング
**ネットワーク環境を学習し、
最適な推奨設定を自動生成**

インパクト解析 攻撃と対象端末情報を解析し本当に危険度の高いログを識別





攻撃の緊急度 “High”のアラート数: 1433

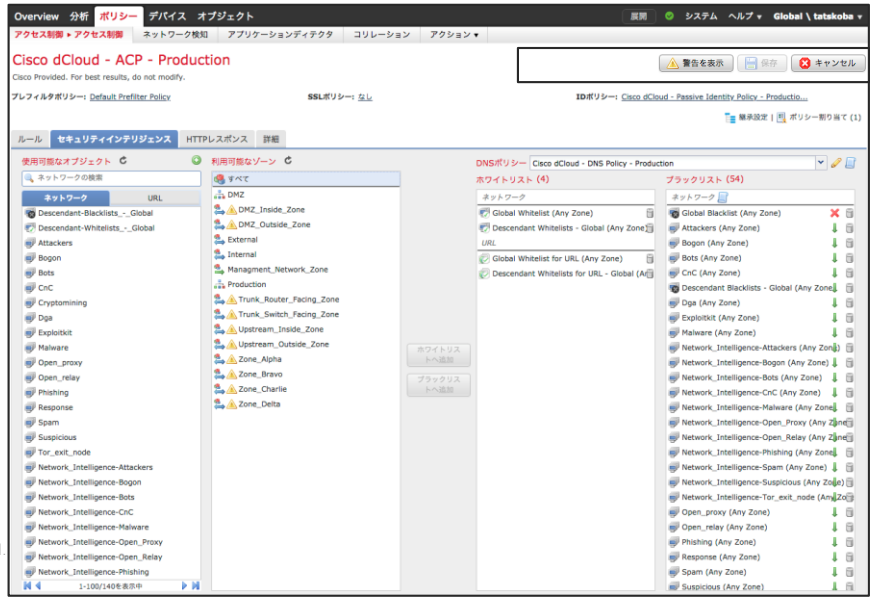
実インパクト “High(1)”のアラート数: 106

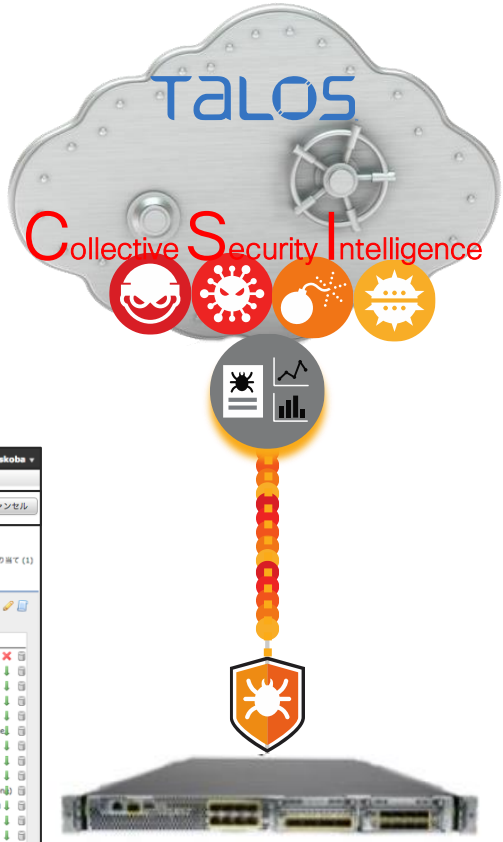
10分の1以下に減少

Security Intelligence 脅威情報フィルタ

- Cisco Collective Security Intelligence 提供のブラックリスト IP アドレス、URL、ドメインに基づく制御 (i.e. レピュテーション)
- 既知のブラックリスト宛て or からのコネクションを　モニターもしくはブロック
- カテゴリー
  - CnC
  - Malware
  - Phishing
  - Bots
  - Attackers

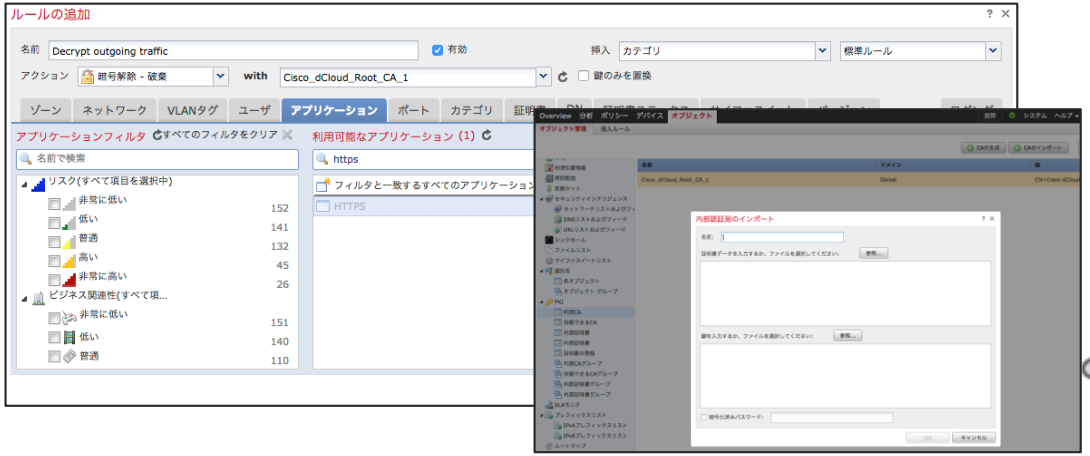
など

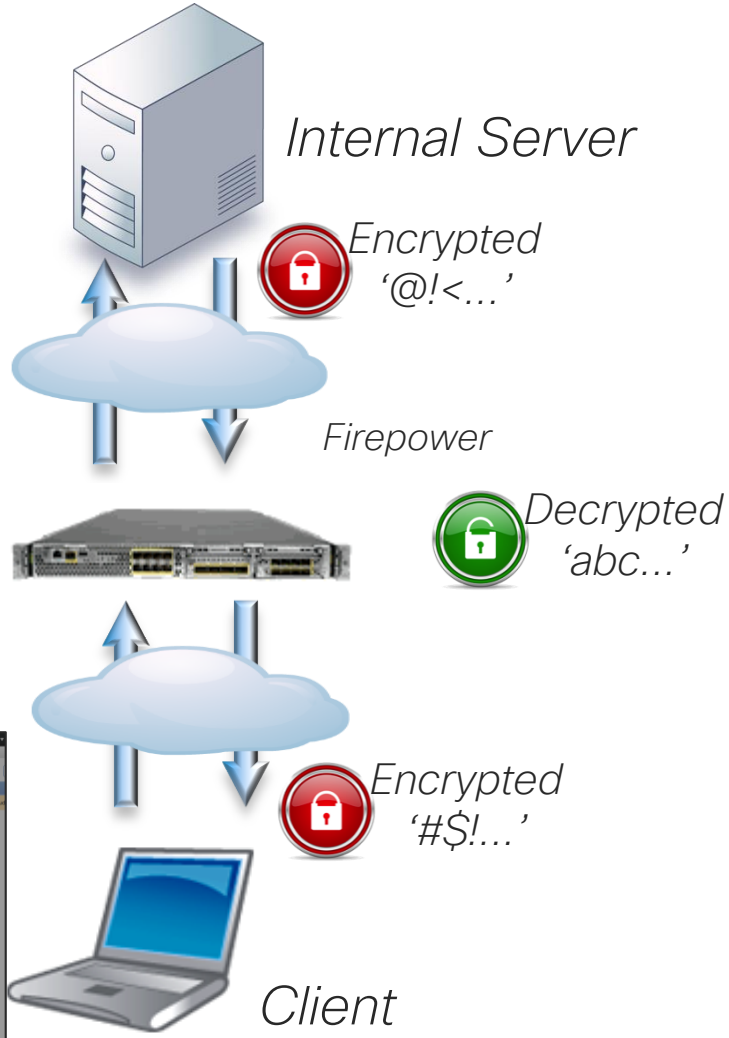




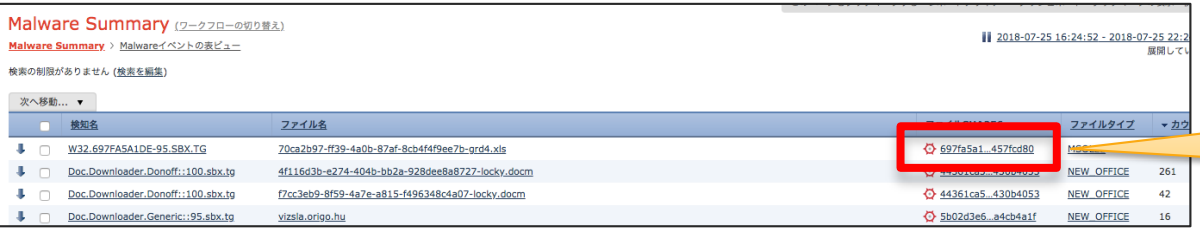
SSL / TLS 復号

- SSL / TLS で暗号化された通信のインスペクションを行う機能
  - inbound passive
  - inbound inline
  - outbound inline
- Version 6.3.0 以降の FP2100/4100/9300 はハードウェア処理となり処理能力が向上

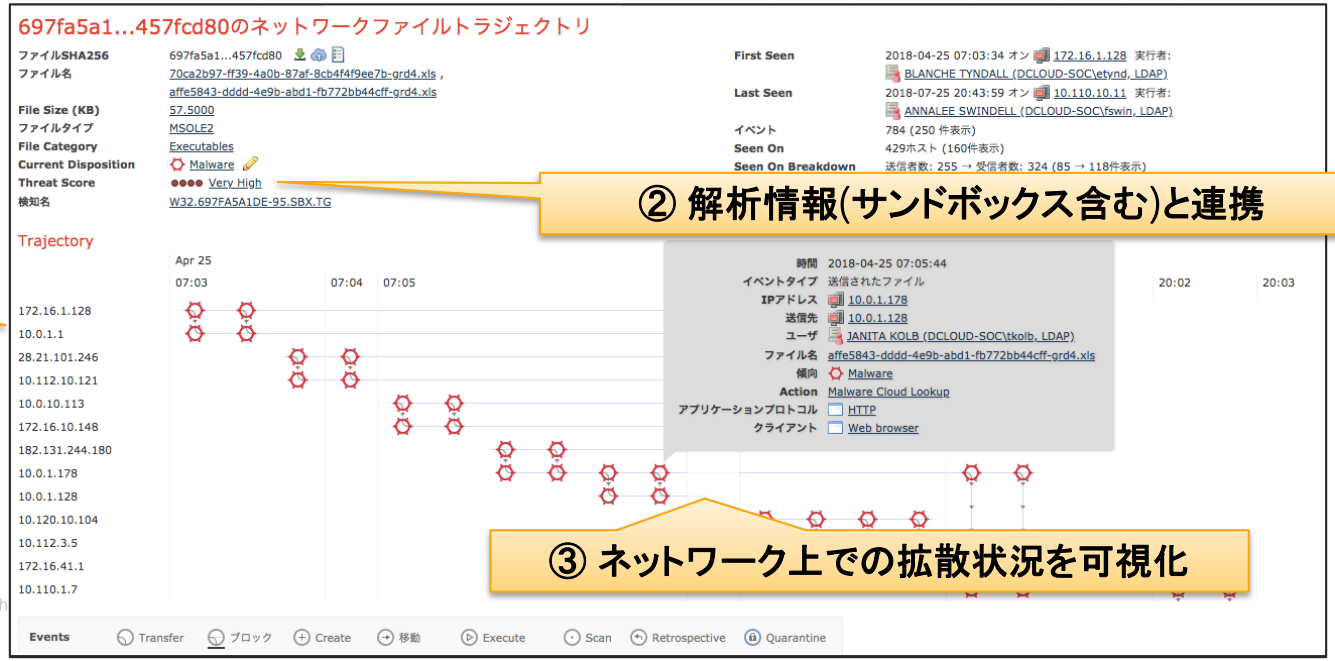




AMP4N (Advanced Malware Protection for Network)
マルウェアの可視化と制御、トラッキング



① ファイルをハッシュ値で特定
(端末で検知したマルウェアもブロック可能)

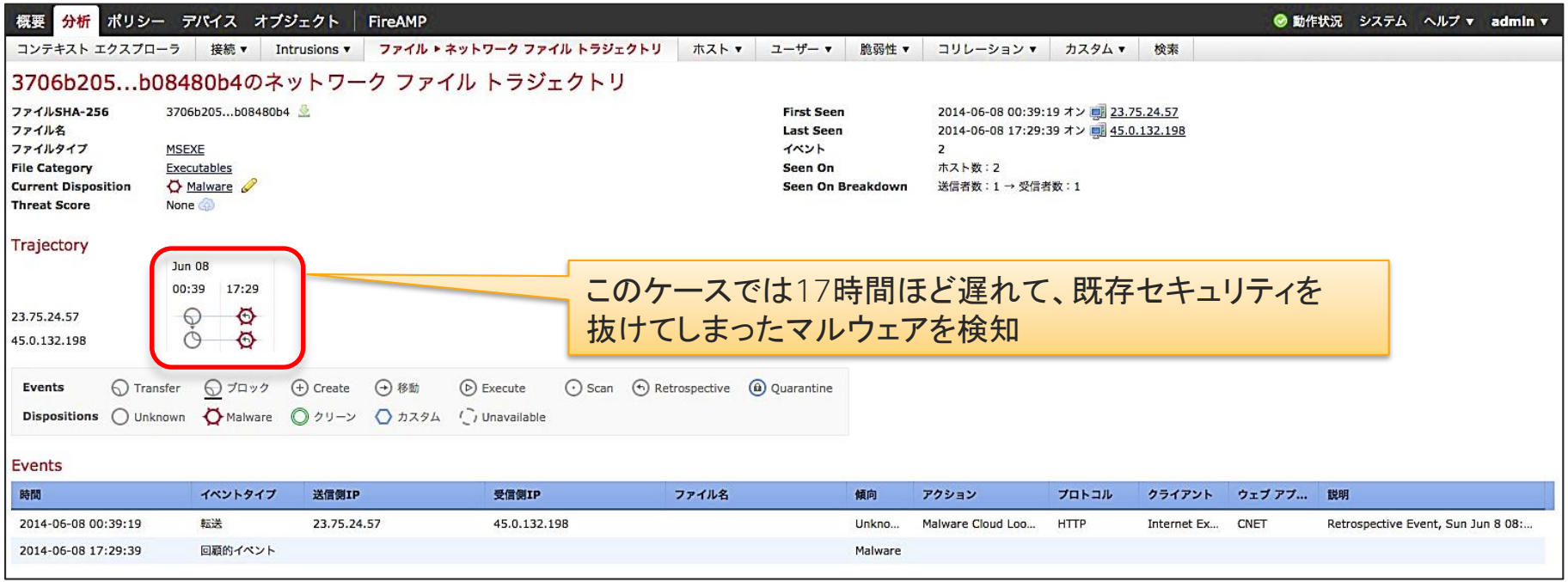


② 解析情報(サンドボックス含む)と連携

③ ネットワーク上での拡散状況を可視化

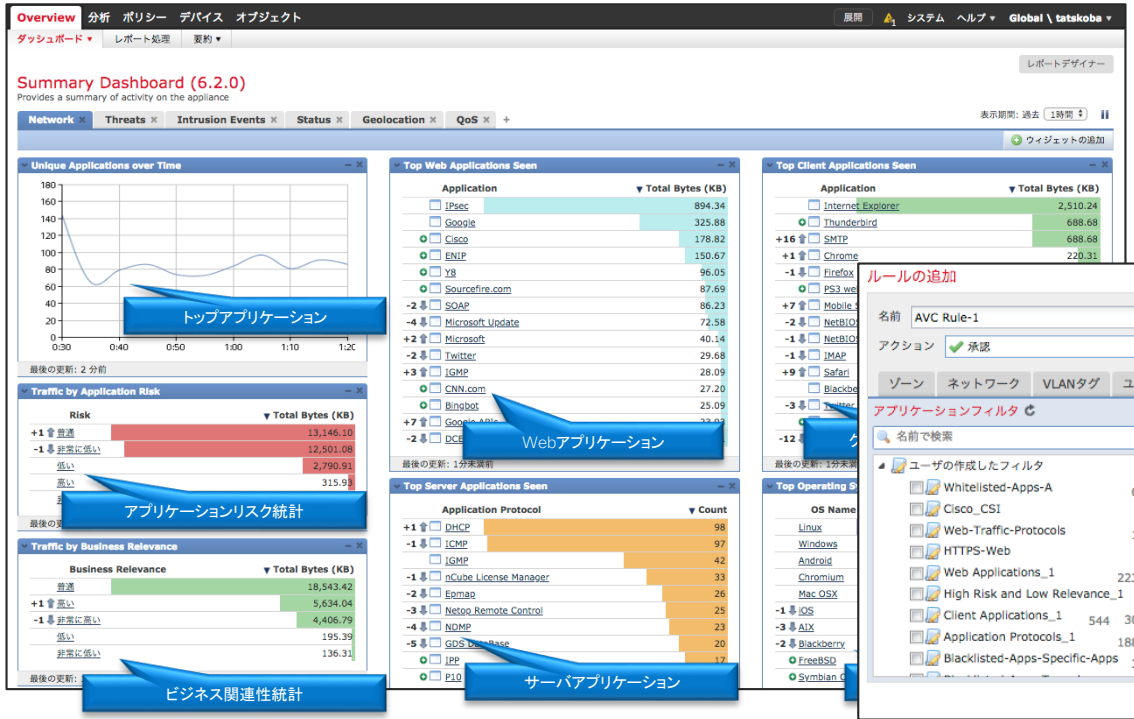
④ 端末の特定

クラウドリコールによるゼロデイマルウェア検知例



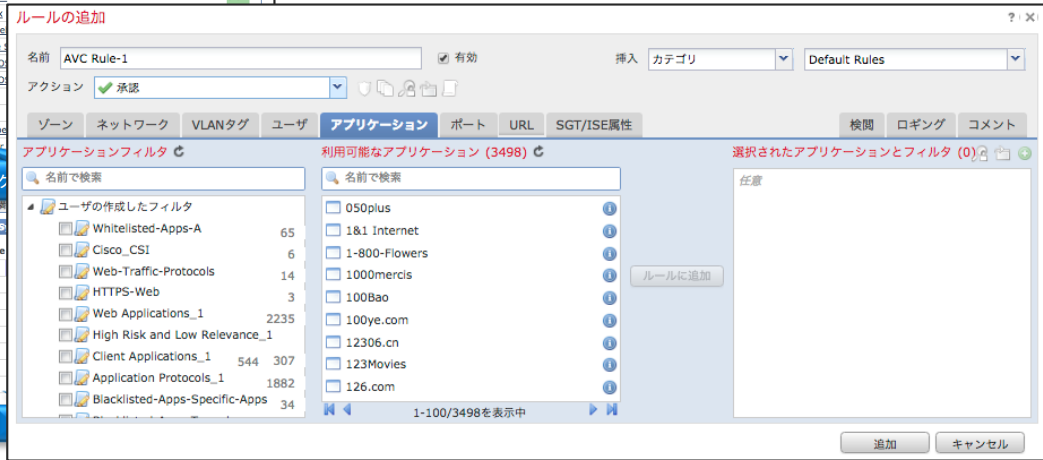
Application Visibility Control アプリケーションの可視化と制御

- 利用されている Web アプリケーション、クライアントアプリケーション、サーバアプリケーション、利用量、リスク統計から、問題点を的確に捉え、アプリケーション制限を実施し、リスクを軽減することが可能



3,500以上（v6.3時点）の アプリケーションから、利用状況をチェック

問題のあるアプリケーション、利用している端末を割り出し、利用の制限を実施し内在するリスクを軽減



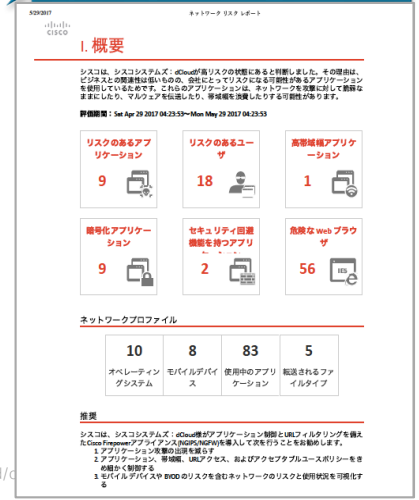
Custom Report レポート機能

柔軟なレポート機能：レポートデザイナ機能でフルカスタマイズ可能

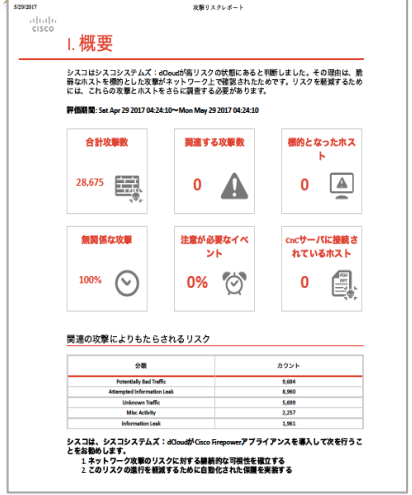
作成したレポートを任意のメールアドレスへ自動転送

PDF、HTML、CSV形式をサポート

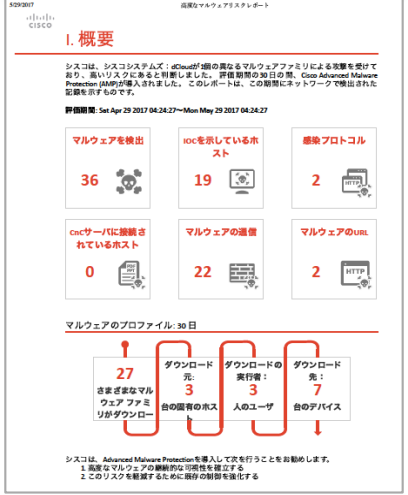
ネットワークレポート



アタックレポート

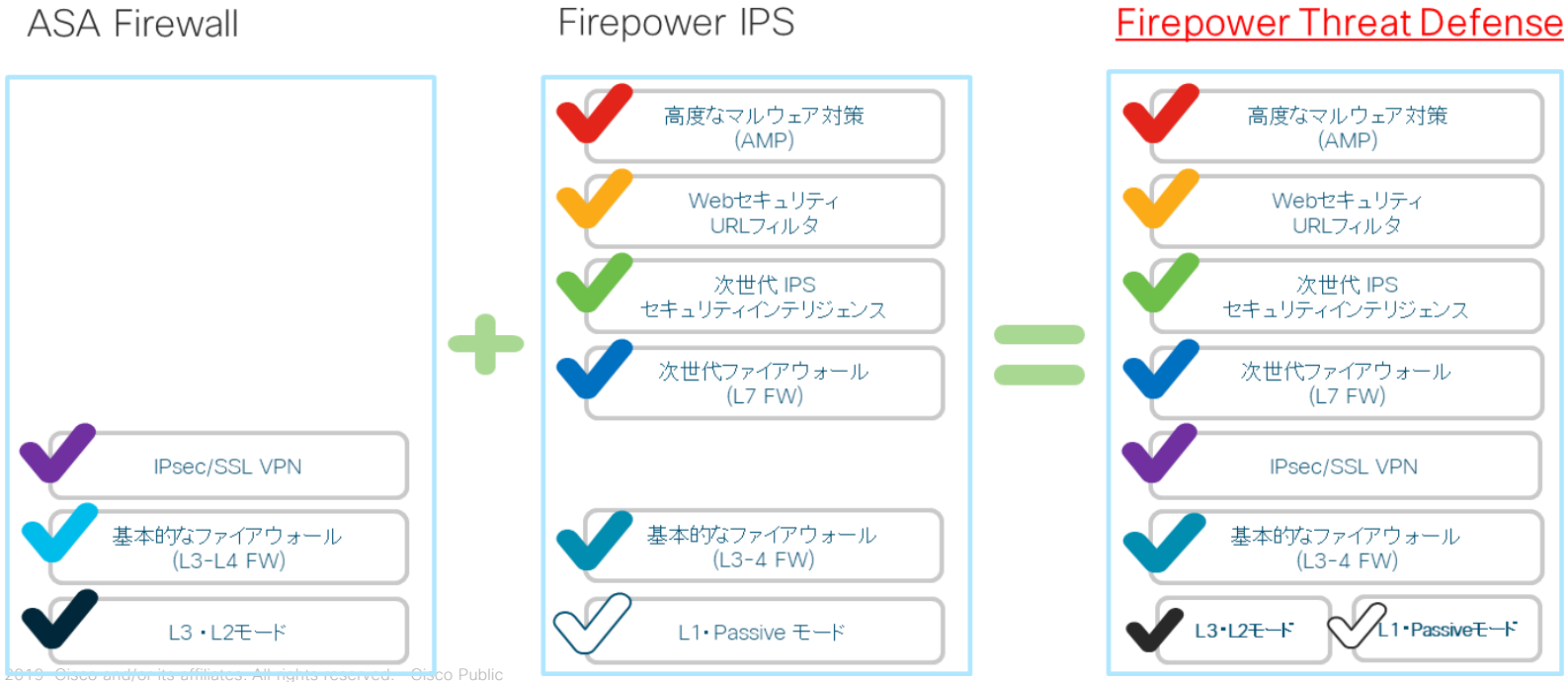


マルウェアレポート



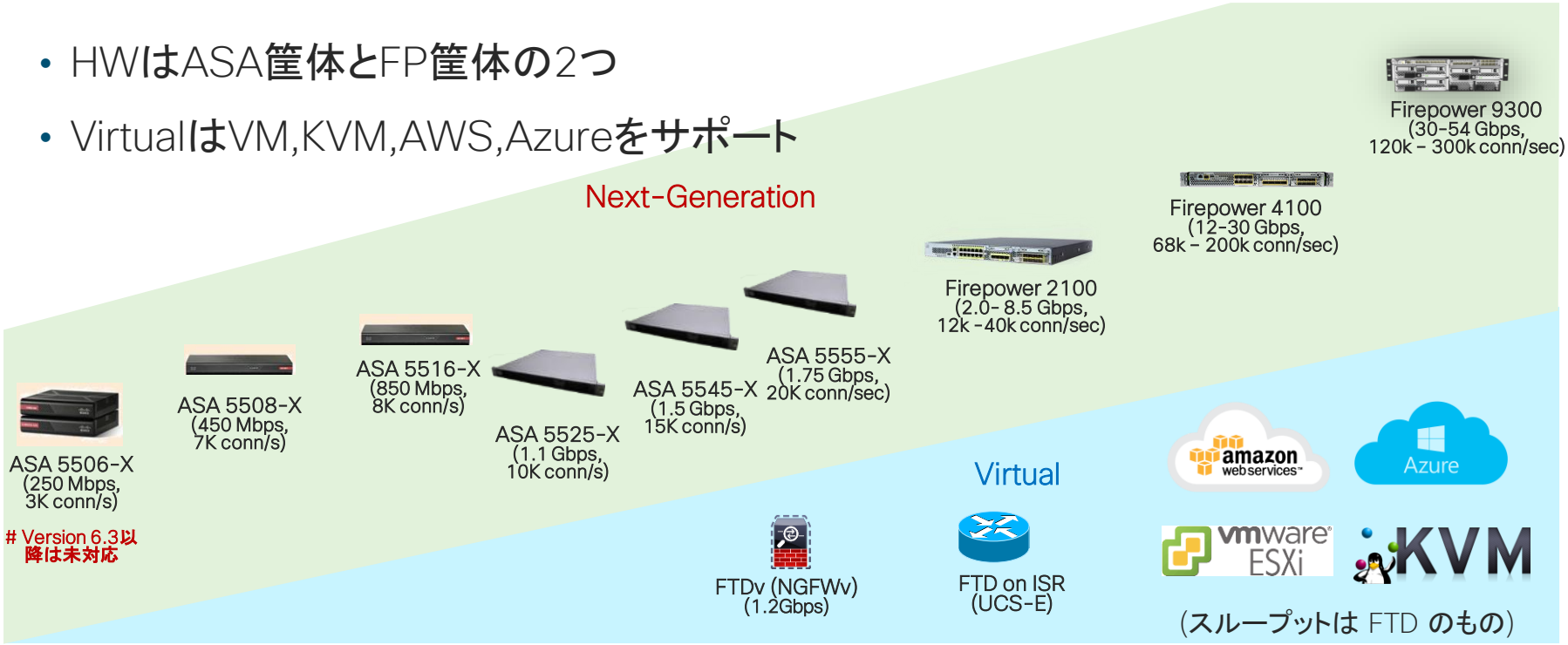
ソフトウェア – Firepower Threat Defense (FTD)

- ASA基本機能とFirepower（NGIPS）を統合した一体型ソフトウェア
- FTDはスマートライセンスが必須



Firepower Threat Defense が動くプラットホーム

- HWはASA筐体とFP筐体の2つ
- VirtualはVM,KVM,AWS,Azureをサポート



※購入後のASA/FTDソフトウェアの入れ替え(リイメージ)可能もライセンスに注意

Off-Box管理 – Firepower Management Center (FMC)

- FTD 管理サーバ(FP41xx/93xx利用時は必須)
- 各種設定・ポリシーの適用と管理・レポートの生成
- ネットワークマップ、IPSルールの自動チューニング やインパクトフラグはFMCで実施
- 日本語対応

FMC

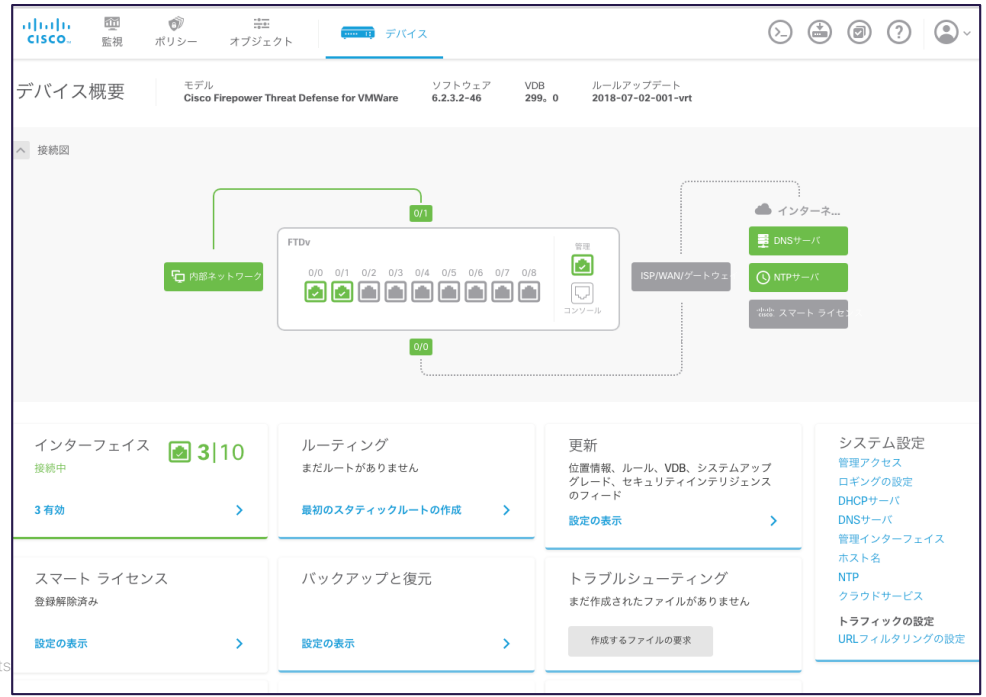
SF Tunnel
互いの Management Interface 間にて TCP/8305 で通信
設定、管理、イベント出力等が行われる

FP Sensor

FTD Virtual 版と FP 専用機 (Virtual 版) を 1台の FMC で管理している例

On-Box管理 - Firepower Device Manager (FDM)

- Web ブラウザで FTD デバイスにアクセス、FTDv,ASA55xx-X,FP21xx で動作
- シンプルなUIで直感的な操作が可能　※ただし機能制限あり
- 日本語対応



Firepower Version 6.3新機能概要

Firepower 6.3.0 新機能一覧

プラットフォームの拡張性

マルチインスタンス for 4100/9300
- 最大14台の仮想インスタンス*
- 冗長構成のサポート

*機種により最大数は異なります。

100GEネットワークモジュール for 9300
- 2x100GE, 4x100GE Module
- シャーシ当たり最大8x100GEまでサポート

HWによるTLS復号化対応
- より高速なTLSインスペクションスループット
- すべてのFirepowerプラットフォームでサポート(2100/4100/9300)

Fail-to-wireネットワークモジュール for FP2100
- 2100でもFTWの利用が可能に

NGIPSからの移行
- 新しいマイグレーションツール

操作性

エアギャップ環境でのライセンス利用
- License Reservationにより、エアギャップ環境でのFTDの利用が可能に

ローカル管理FTDの機能拡張
- ハイアベイラビリティ、パッシブ認証、SmartCLI(Routing、ACL等)、RAVPN認証関連等

FMCで管理されている全FTDのフルバックアップが可能に

Syslogイベントの統合
- ASAとSnortからまとめて一つのSyslogを送信

可視性＆セキュリティ

イベントログから他製品との容易な連携
- 他のCisco製品やサードパーティSIEMsとのシームレスな統合

FQDN ベースのアクセスコントロール
- ASA機能のFTDへのマイグレーション
- 動的クラウドベースアプリケーションのためのコントロール有効化

FMCにおける2FA & RADIUS CoA for RA VPN
- ASA機能のFTDへのマイグレーション

Firepower 6.3.0 新機能一覧

今回のLabで操作可能な機能

プラットフォームの拡張性

マルチインスタンス for 4100/9300
- 最大14台の仮想インスタンス*
- 冗長構成のサポート

*機種により最大数は異なります。

100GEネットワークモジュール for 9300
- 2x100GE, 4x100GE Module
- シャーシ当たり最大8x100GEまでサポート

HWによるTLS復号化対応
- より高速なTLSインスペクションスループット
- すべてのFirepowerプラットフォームでサポート(2100/4100/9300)

Fail-to-wireネットワークモジュール for FP2100
- 2100でもFTWの利用が可能に

NGIPSからの移行
- 新しいマイグレーションツール

操作性

エアギャップ環境でのライセンス利用
- License Reservationにより、エアギャップ環境でのFTDの利用が可能に

ローカル管理FTDの機能拡張
- ハイアベイラビリティ、パッシブ認証、SmartCLI(Routing、ACL等)、RAVPN認証関連等

FMCで管理されている全FTDのフルバックアップが可能に

Syslogイベントの統合
- ASAとSnortからまとめて一つのSyslogを送信

可視性＆セキュリティ

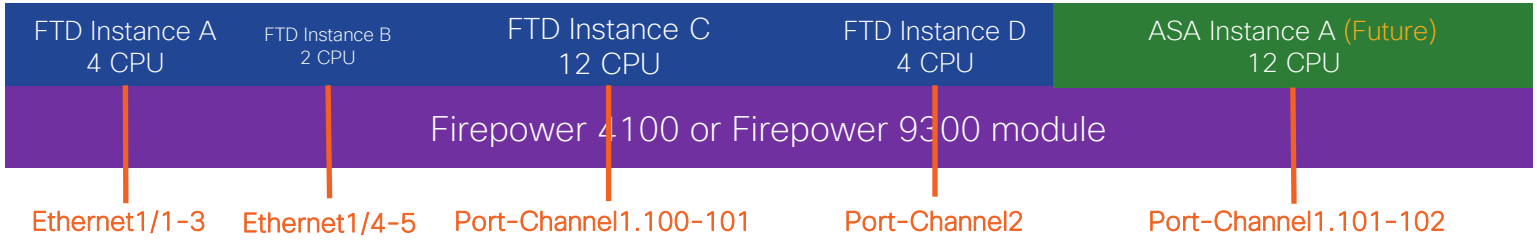
イベントログから他製品との容易な連携
- 他のCisco製品やサードパーティSIEMsとのシームレスな統合

FQDN ベースのアクセスコントロール
- ASA機能のFTDへのマイグレーション
- 動的クラウドベースアプリケーションのためのコントロール有効化

FMCにおける2FA & RADIUS CoA for RA VPN
- ASA機能のFTDへのマイグレーション

参考）マルチインスタンスの概要

- Firepower 4100 と 9300 **のみでサポート**
- 1つのモジュール or アプライアンスで複数の論理デバイスが稼働
  - まずは FTD のみでサポート、FTD と ASA の混在は**将来サポート予定**
  - Docker インフラとコンテナのパッケージングを活用
- トラフィックも管理も完全に分離
- 物理/論理インターフェイスと VLAN は Supervisor で実施



参考）マルチインスタンスの利点

- Network Security 製品におけるユニークで新しいアプローチ
- ハードウェアレベルでのトラフィックの処理と管理プロセスの完全な分離
- シングルコンテキストで完結する機能はすべてサポート
- ソフトウェア管理や再起動を完全に独立して実施可能
- 将来は FTD と ASA のインスタンスの共存が可能
- 将来はハードウェアから Docker コンテナとして FTD と ASA を持ち出し可能
- 品質と導入コストの双方にメリット

参考）Airgap 環境での FTD ライセンス

- FTD は必ずスマートライセンスが必要
- FMC の管理インターフェイスからインターネットにアクセス不可な環境ではスマートライセンスサテライトサーバにて対応
- スマートライセンスサテライトサーバの利用が何らかの理由で不可能な場合には、FTD 6.3.0 からサポートされる以下のどちらかを選択し、事前にシスコからの承認を得る必要がある。いずれもインストール時に Cisco Smart Software Manager (CSSM) に管理者がアクセスし、ライセンスを確保することで、FMC からの定期的な CSSM へのアクセスを省くことが可能
  - UPLR – Universal Permanent License Reservation

    全機能が利用可能なため、利用については厳密な審査が行われる
  - SLR – Specific License Reservation

    機能を選択して利用可能、UPLR ほど厳密ではないが、事前に申請が必要
- どの選択を行ってもスマートアカウントの作成、利用は必要なことに注意

参考）品質のさらなる向上 – Snort リスタート 機能改善

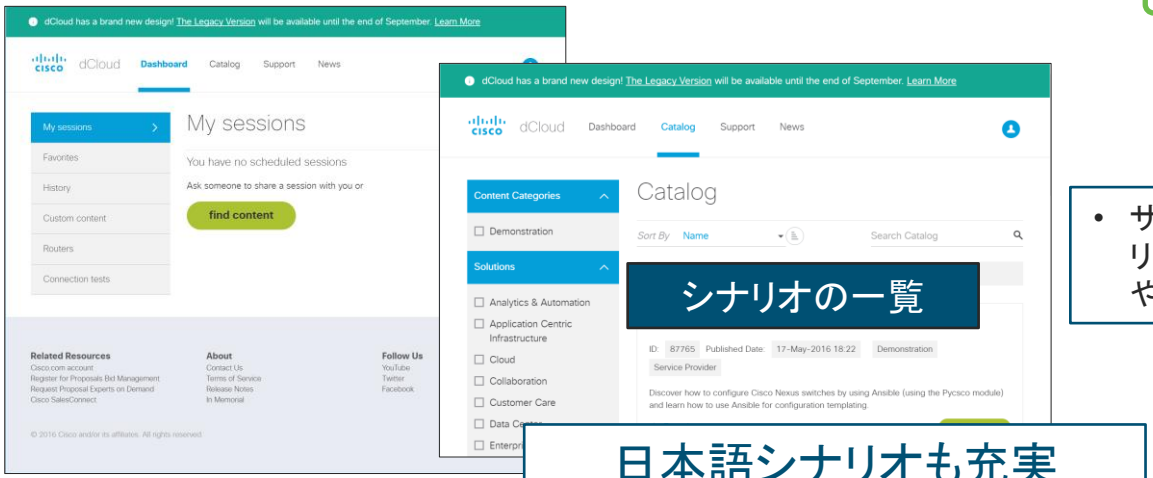
- 6.3.0 にてさらにいくつかのシナリオにて Snort リスタートが不要に
  - テキストに加えてバイナリのルールも含めたすべての SRU
  - 実際にデプロイする前の VDB 更新インストール
- Snort リスタートが起きるシナリオは、あとはこれだけ
  - Talos が関係しない VDB 更新やカスタムアプリケーションディテクタの変更
  - File Policy のオプション変更 (Snort のインスタンス数が変わる際のみ)
  - TLS or Captive Portal Policy の有効化/無効化
  - HA ペアの作成/破棄時
  - Network Discovery での Traffic-Based Detection で HTTP, FTP, or MDNS の有効化/無効化
  - 全データインターフェイスでの最大 MTU の変更

dCloud利用方法

dCloud (Demo Cloud)

http://dcloud.cisco.com/

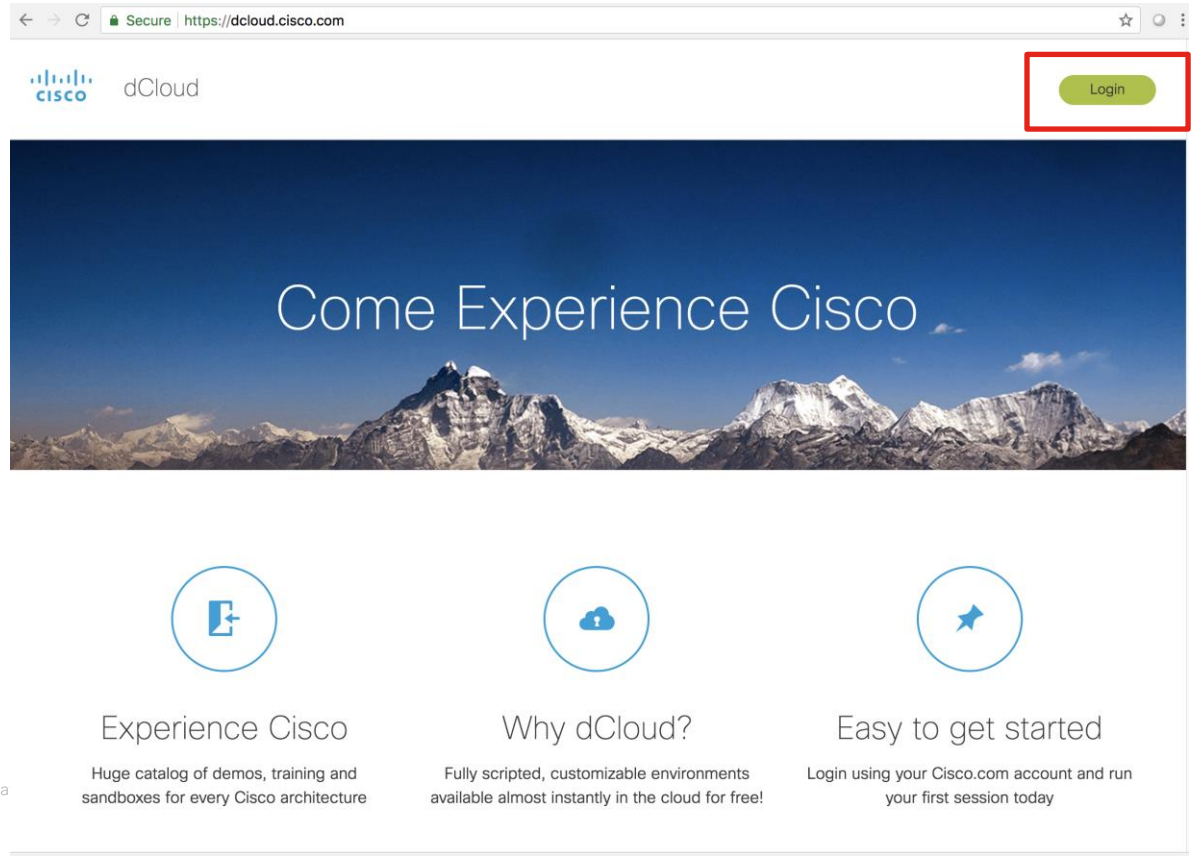
いつでもどこでもインターネット経由で呼び出せる「**デモ環境**」、「**PoV環境**」、「**ラボ環境**」です。
デモ環境はセットアップ済で提供されるため、すぐにデモができるため、準備 (機材の入手やセットアップ、シナリオ作成) にかかる時間が省略できます。



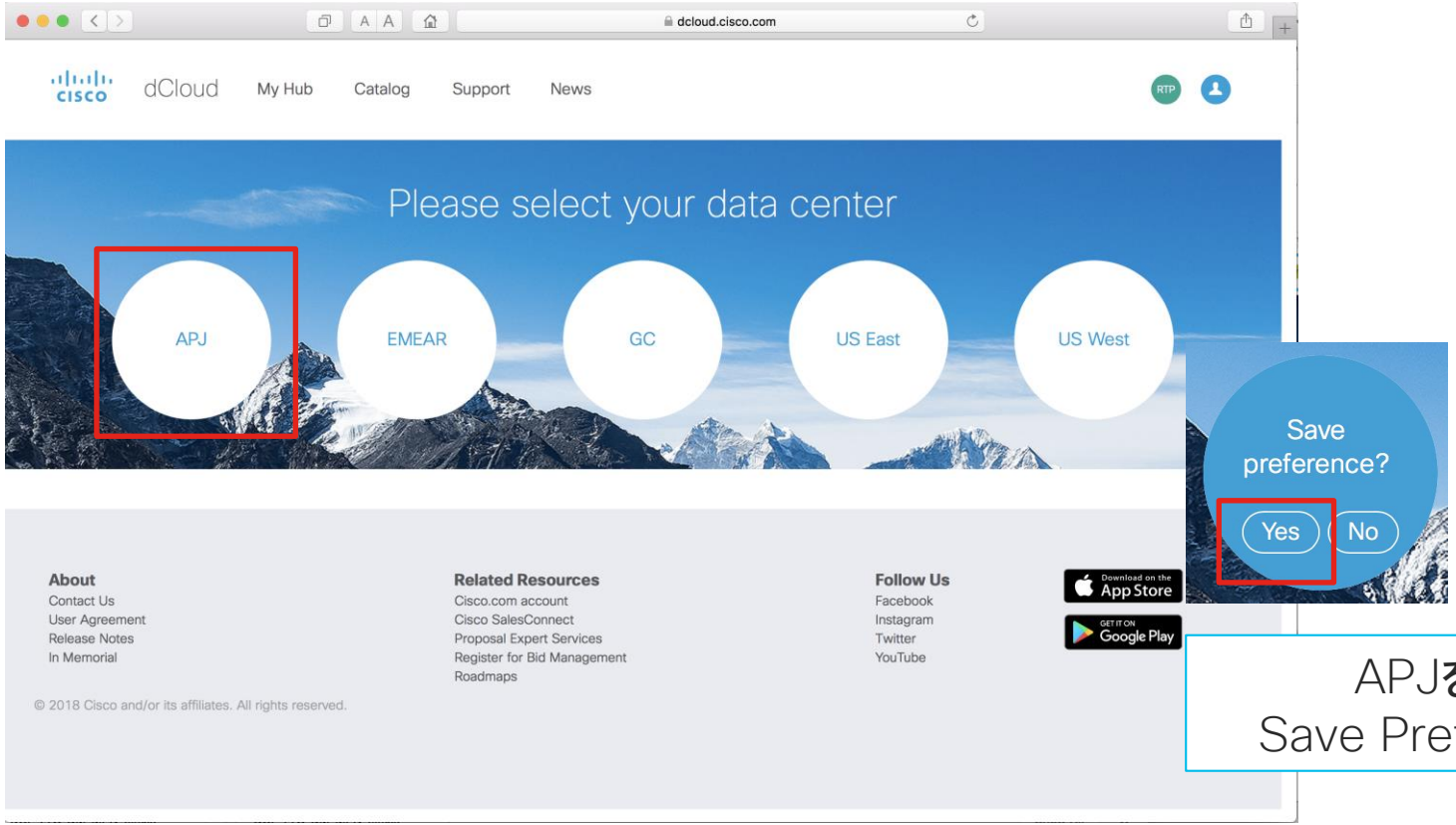
- サポートコミュニティの “システムズエンジニアリング” の項目で、dCloud に関するコンテンツや使い方などを紹介しています。

日本語シナリオも充実

dcloud.cisco.comへアクセスし、ログインをクリック



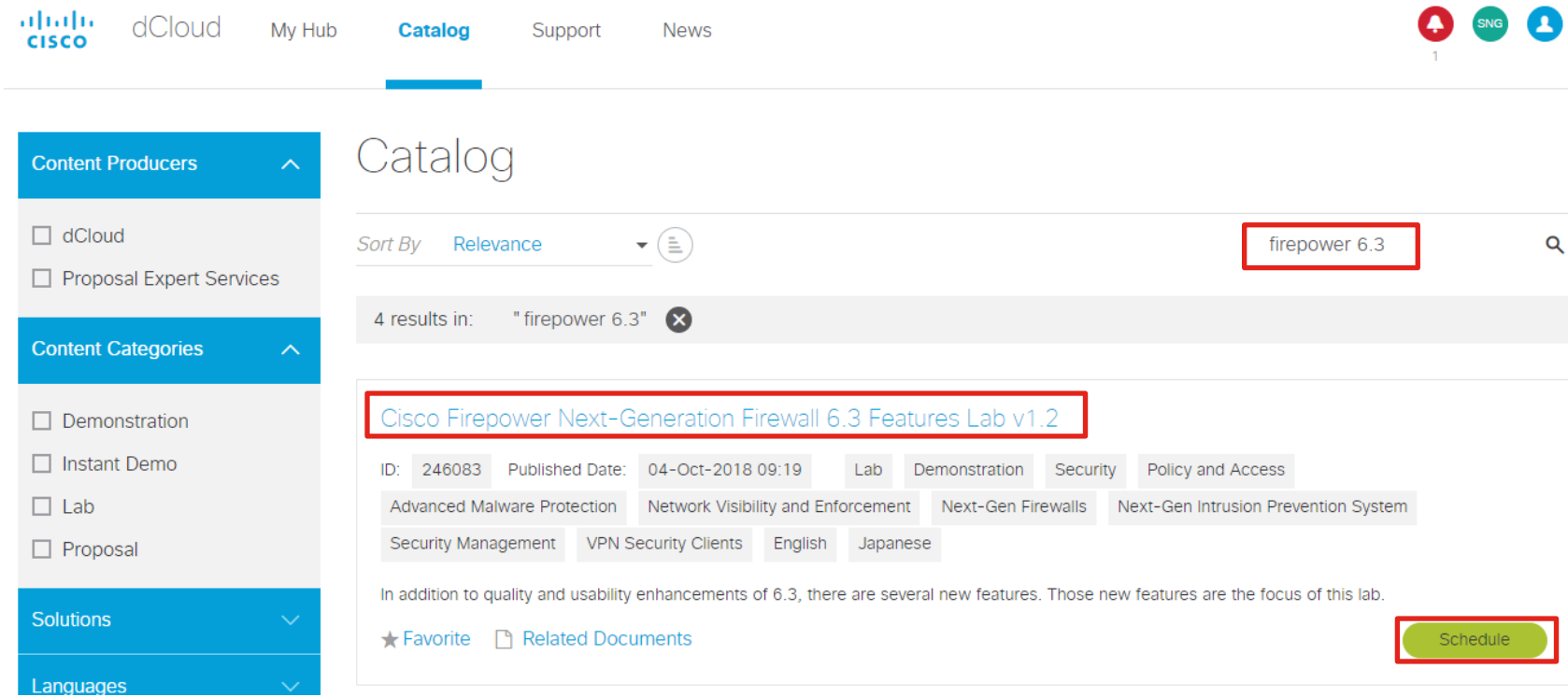
初回のみ：通常利用のデータセンタの指定



APJを選択し、
Save PreferenceでYes

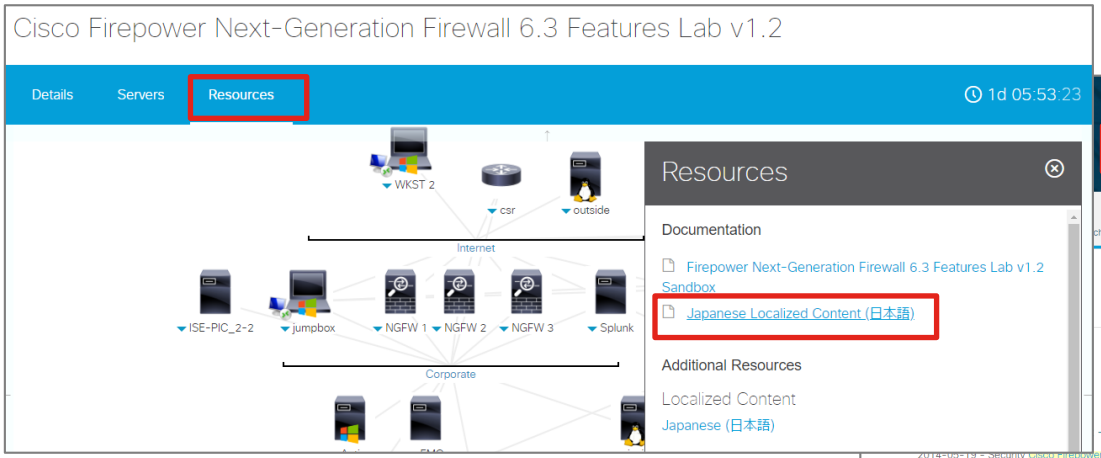
ラボ予約

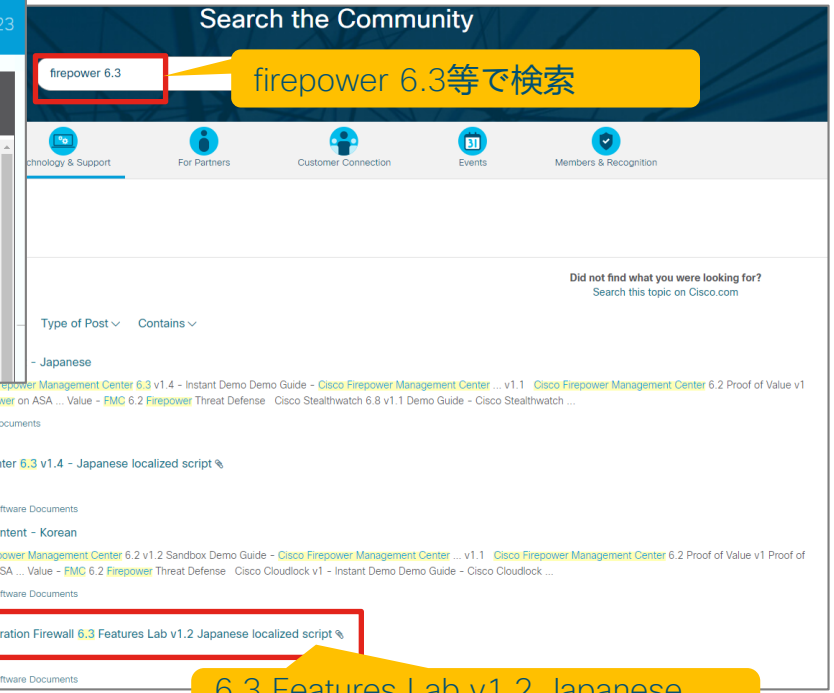
Catalogから”Firepower 6.3”で検索し、”Cisco Firepower Next-Generation Firewall 6.3 Features Lab v1.2”をスケジュール



ラボ資料

スケジュールされたラボを選択し、Resourcesから”Japanese Localized Content（日本語）”をクリックして日本語の資料をダウンロード

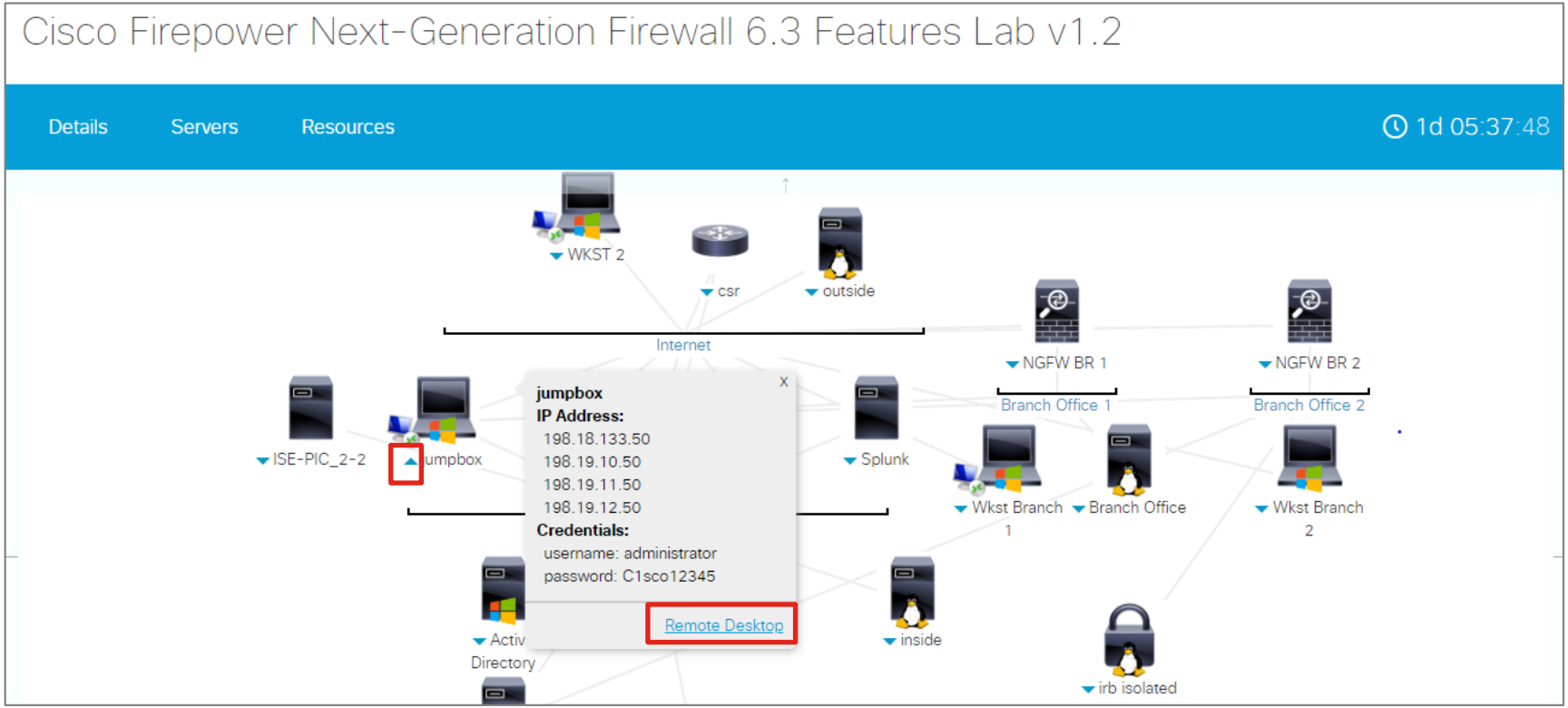




ラボへのアクセス方法 (1)

※(1)か(2)のいずれか

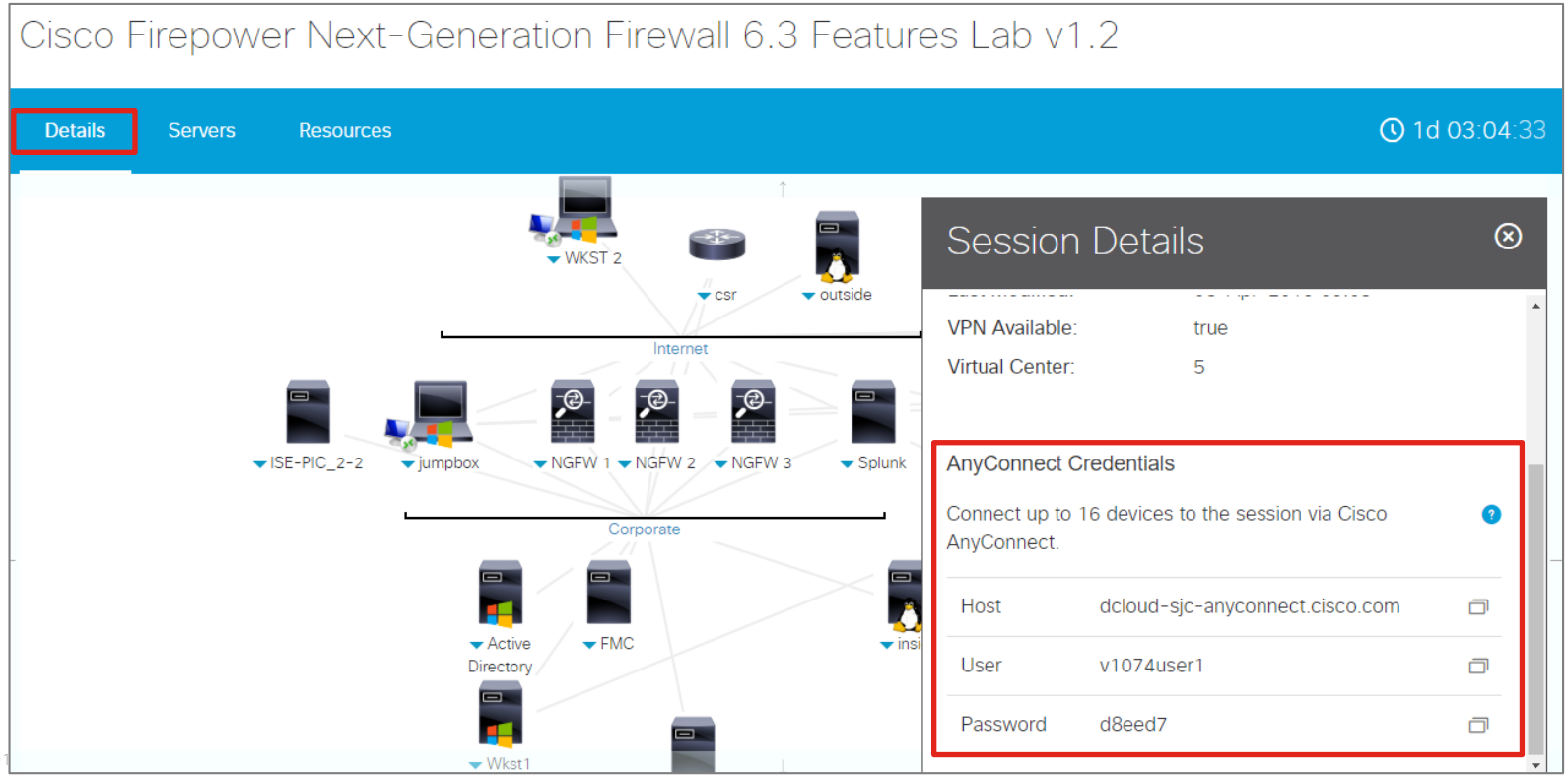
Jumpboxメニューを展開し、Remote Desktopをクリック



ラボへのアクセス方法 (2)

※(1)か(2)のいずれか

DetailsタブのAnyConnect Credentialsを利用してAnyConnectでリモート接続を行い、jumpboxに直接リモートデスクトップ接続



ラボシナリオのご紹介

ラボシナリオ

※FDMシナリオとFMCシナリオは独立していますので
どちらか片方のみでもお試し可能です

FDMシナリオ
シナリオ1：FDM変更管理、RBAC、スマートCLIを使用したBGP設定
シナリオ2：FDMパッシブ認証、FQDN型オブジェクト
シナリオ3：FDM高可用性

FMCシナリオ
シナリオ4：統合イベント、状況に応じた相互起動、FQDN型オブジェクト
シナリオ5：リモートアクセスVPNの認可変更
シナリオ6：RMAのためのバックアップと復元

ラボシナリオ

FDMシナリオ
シナリオ1：FDM変更管理、RBAC、スマートCLIを使用したBGP設定
シナリオ2：FDMパッシブ認証、FQDN型オブジェクト
シナリオ3：FDM高可用性

FMCシナリオ
シナリオ4：統合イベント、状況に応じた相互起動、FQDN型オブジェクト
シナリオ5：リモートアクセスVPNの認可変更
シナリオ6：RMAのためのバックアップと復元

Firepower Device Manager (FDM) の機能拡張

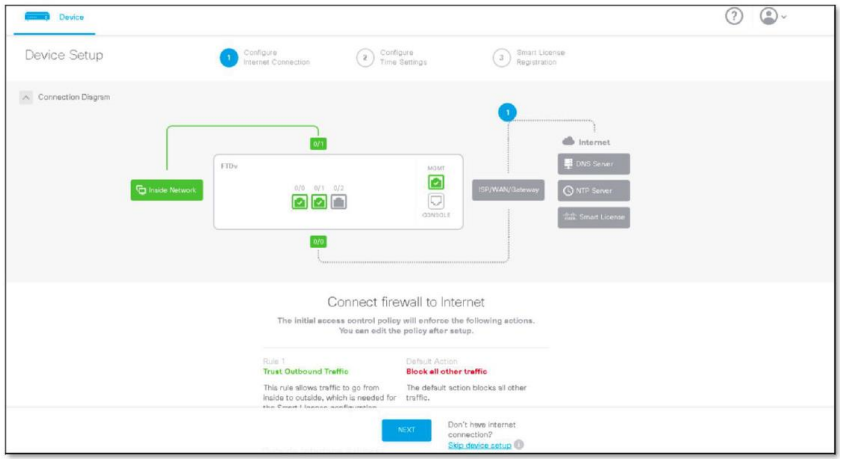
- FTD High Availability
- Passive Interfaces
- Passive Identity rules (ISE-PIC のみサポート)
- SmartCLI: BGP Routing; OSPF2 Route Map, Prefix List, ACL
- RAVPN 用のローカルユーザ DB, Access & TLS Policies
- RAVPN: 二要素認証や証明書認証を伴う RADIUS 認証
- RBAC (R/O, R/W, Admin roles) を伴う外部 RADIUS 認証
- 管理機能の追加: Pending Preview/Copy/Discard, Audit/History

シナリオ1： FDM変更管理、RBAC、スマートCLIを使用したBGP設定

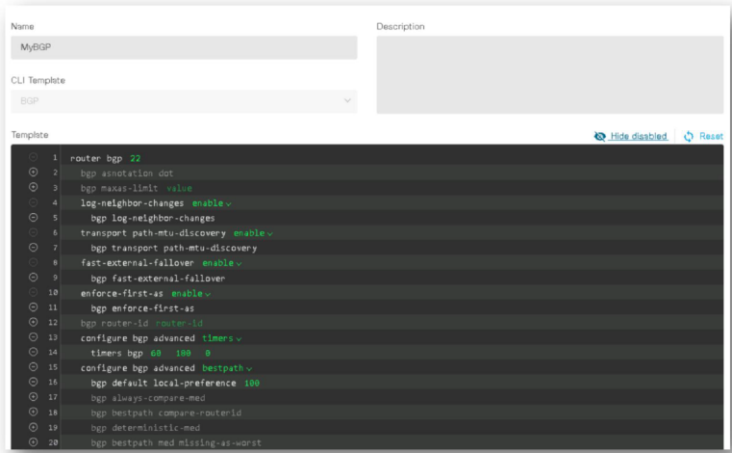
本シナリオでの体験内容

- FDMでの初期セットアップおよび基本設定
- FDM　スマートCLIを使用したBGPの設定とテストの実施
- FDMでのRADIUS認証を使用したロールベースアクセス制御の設定とテストの実施

FDM



スマートCLI

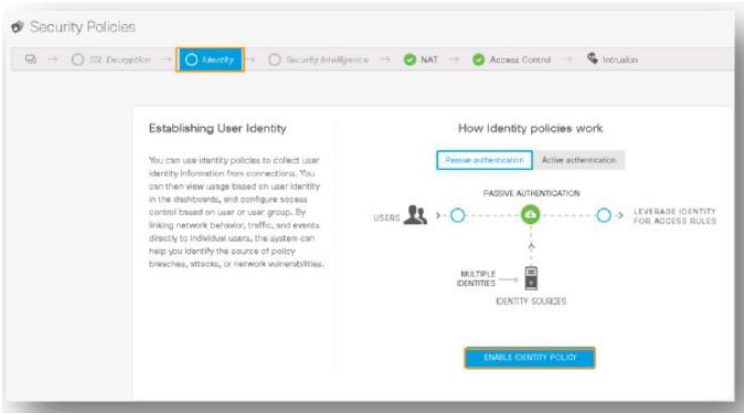


シナリオ2： FDMパッシブ認証、FQDN型オブジェクト

本シナリオでの体験内容

- FDMでのパッシブ認証の設定
- FDMでのFQDN型オブジェクトとアクセスポリシーの作成
- ユーザーアイデンティティおよび宛先FQDNに渡されたトラフィックアクセスのテスト

パッシブ認証



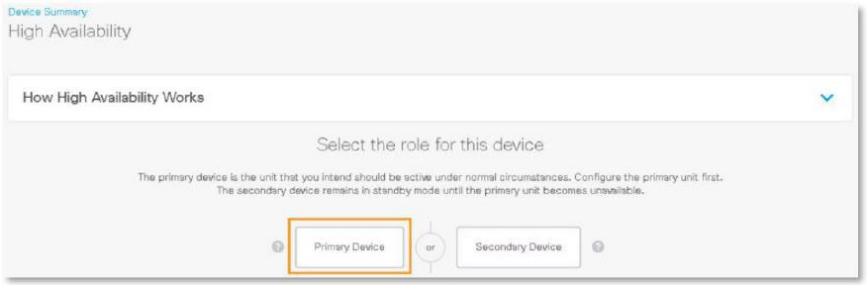
FQDN型オブジェクトを利用したアクセスポリシー（イメージ）

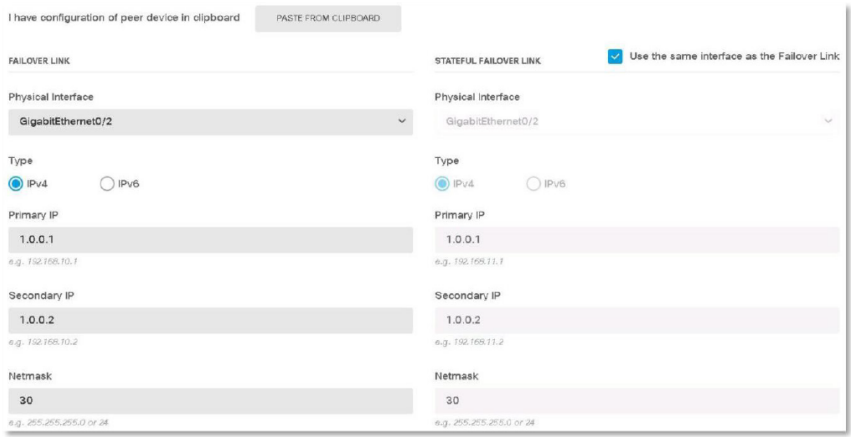
シナリオ3： FDM高可用性

本シナリオでの体験内容

- FDMでのHA（Active/Standby）設定
- FailoverおよびHA解除のテスト

FDMでのHA設定画面





注意！シナリオ3： FDM高可用性　ラボ資料の誤りについて

P.41　NGFW3のHA設定手順にて以下の記述ミスがあります。

誤： 9. このデバイスの HA ロールとして [プライマリデバイス（Primary Device）] を選択します。
正： 9. このデバイスの HA ロールとして [セカンダリデバイス（Secondary Device）] を選択します。

※誤って設定してしまった場合にはHA設定画面内の  より
Break HAを選択し、HA構成を一旦解除して再設定ください

ラボシナリオ

FDMシナリオ
シナリオ1：FDM変更管理、RBAC、スマートCLIを使用したBGP設定
シナリオ2：FDMパッシブ認証、FQDN型オブジェクト
シナリオ3：FDM高可用性

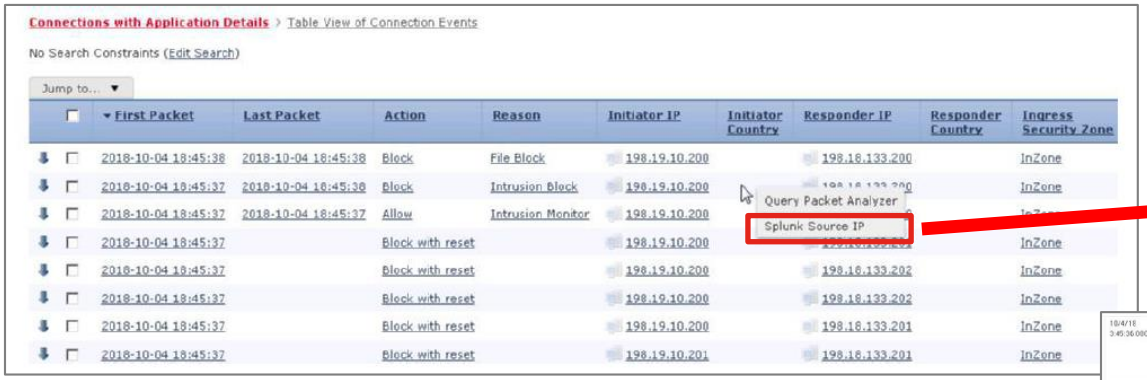
FMCシナリオ
シナリオ4：統合イベント、状況に応じた相互起動、FQDN型オブジェクト
シナリオ5：リモートアクセスVPNの認可変更
シナリオ6：RMAのためのバックアップと復元

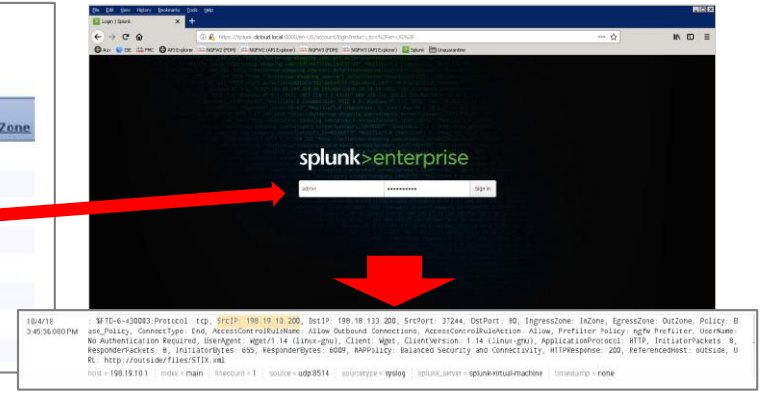
シナリオ4：統合イベント、状況に応じた相互起動、FQDN型オブジェクト

本シナリオでの体験内容

- FMCでのFQDN型オブジェクトを使用したアクセスポリシーの設定とSyslogサーバー（Splunk）への接続イベント送信設定
- FMCでのSplunkとの相互起動設定とテスト

SplunkとのContextual Cross-launch

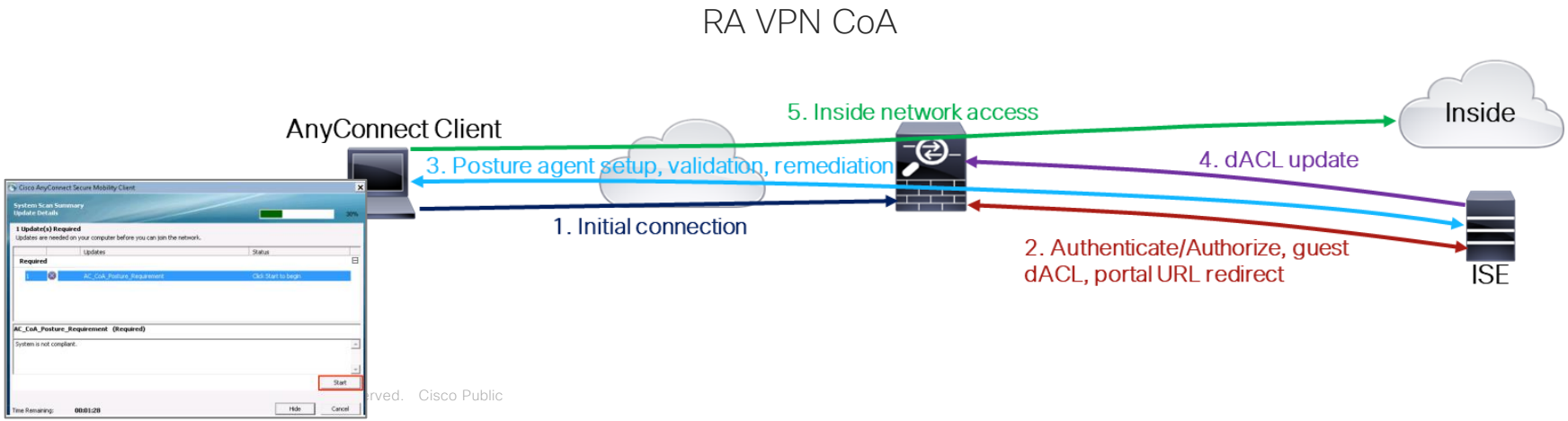




シナリオ5：リモートアクセスVPNの認可変更

本シナリオでの体験内容

- FMCでのリモートアクセスVPNのポスチャ評価と認可変更（Change of Authorization）に必要なオブジェクトの作成
- FMCでのリモートアクセスVPNセットアップウィザードの実行
- リモートアクセスVPNのポスチャ評価と認可変更のテスト



シナリオ6：RMAのためのバックアップと復元

本シナリオでの体験内容

- FMCで管理されているFTD（NGFW1）のバックアップ取得
- NGFW1号機のシャットダウン（障害シミュレート）
- 別FTD筐体（NGFW3）への復元

6.3ではFTDのデバイス設定（インターフェースやルーティング設定等）を含むバックアップ取得が可能となった

注意点：

- クラスタ構成は未サポート
- FP4100/9300のFXOS部分は個別のバックアップが必要
- FMCよりバックアップオペレーションを実施し、リトリーブは各デバイスで実施
- リストアのオペレーションは各デバイスで実施
- リストアにおいてHWモデル、SWバージョン、VDBバージョンを一致していなければならない
- FlexconfigやVPN設定はマニュアルでの再設定が必要になる場合がある（警告メッセージが表示）
- リストア後、証明書は再エンロールメントが必要

参考資料 (1)

- Firepower への cisco.comでのショートカット

  http://www.cisco.com/go/ngfw

- パートナーサポート
  - 最新資料 (FTD 初期設定ガイド、ASA on FP4k2k ガイド公開中)

    https://www.cisco.com/c/m/ja_jp/partners/documents.html
  - セキュリティ技術資料

    https://www.cisco.com/c/ja_jp/partners/sell-integrate-consult/technology/security.html

- シスコサポートコミュニティ 日本語 セキュリティ

  https://community.cisco.com/t5/-/ct-p/5041-security

参考資料 (2)

- シスコシステムズ合同会社 コーポレートブログにて、Firepower 6.3.0 の機能解説を、3回に渡って掲載
  - 新機能満載の Cisco Firepower 6.3.0 をリリースしました その1
    https://gblogs.cisco.com/jp/2018/12/fp630-release-1/
  - 新機能満載の Cisco Firepower 6.3.0 をリリースしました その2
    https://gblogs.cisco.com/jp/2018/12/fp630-release-2/
  - 新機能満載の Cisco Firepower 6.3.0 をリリースしました その3 (最終回)
    https://gblogs.cisco.com/jp/2018/12/fp630-release-3/


CISCO