RedSeal
初期導入
サーバー構築概要

RedSeal サーバー構築工程の概要

- Data Collection
  - コンフィグファイルの収集
- Best Practice Checks
  - コンフィグファイルの精査
- Topology Layout
  - トポロジーマップの生成
  - グループの定義とネットワーク構成図の作成
- Model Issues
  - モデルの整合性の確認
- Threat Sources
  - インターネット等の信頼性が低いサブネットの定義
- Analysis
  - 分析を実施
- Access Queries
  - アクセスパスの検証
- Security Segmentation (Zones & Policy)
  - セグメンテーションの確認とポリシーの定義
- Vulnerability Management
  - 脆弱性のアクセスパス分析と優先付け
- Security Intelligence Center – Security Impact Query
  - 可視化されたネットワークのセキュリティを検証

Data Collection

- コンフィグファイルの収集作業
  - 次の収集方法がある
    - 実機アクセス（RedSealがssh等でインタラクティブにログインし、コンフィグを集める）
    - CMDB（構成管理データベース）から収集
    - ネットワークファイルサーバーに保存されているコンフィグファイルを収集
    - 手動でコンフィグを集め、インポートする
  - 備考
    - 本番ネットワークではコンフィグファイル収集を自動化する事を推奨
      - 通常毎日行われる
      - チェンジマネージメントに合わせて収集するシナリオもある
    - 脆弱性スキャナの出力があればコンフィグファイルと同じやり方で取り込む

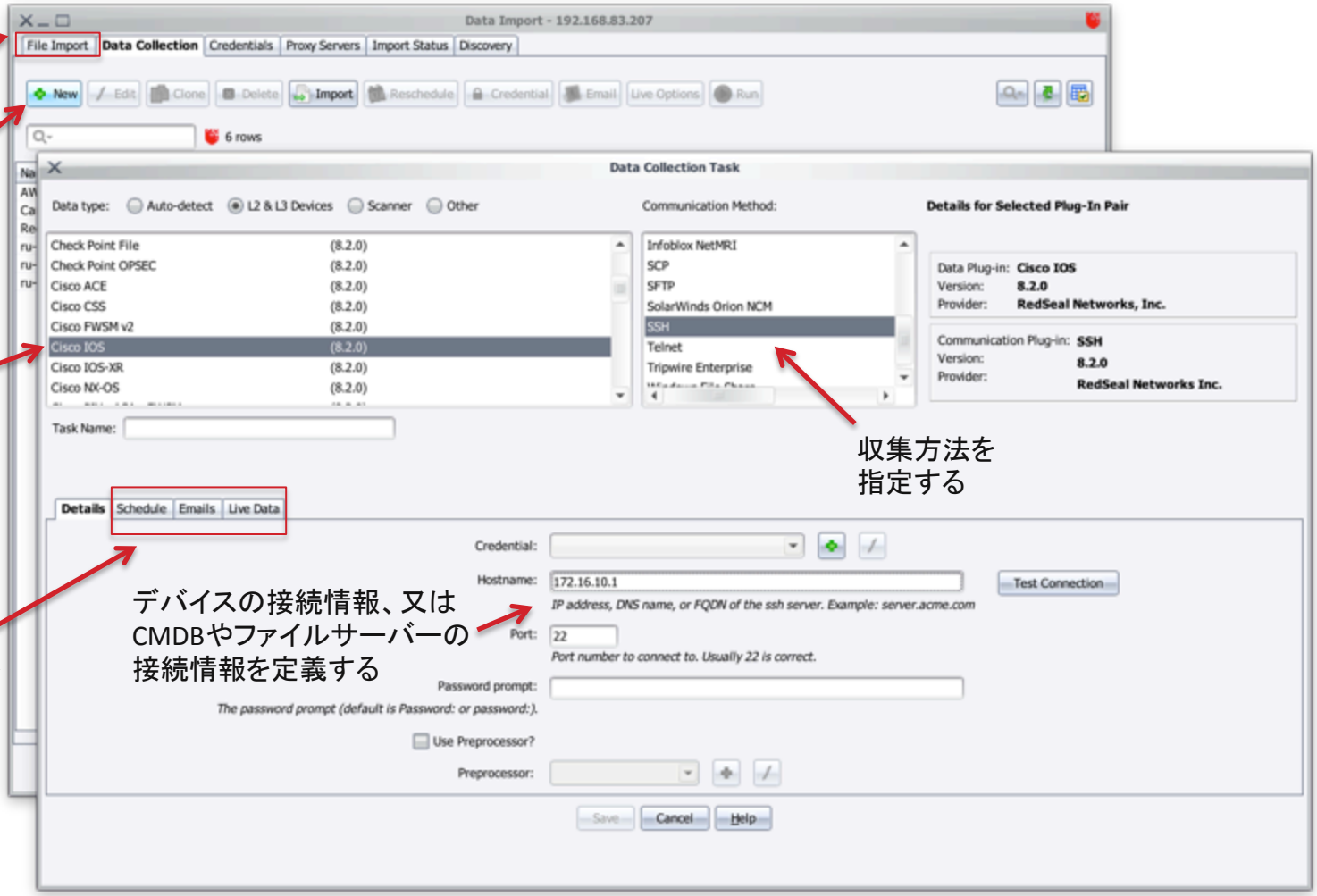
Data Collection

手動でコンフィグファイルをインポートする場合

実機アクセス、CMDB、又はファイルサーバーからコンフィグファイルを収集する場合

デバイスタイプを指定する（脆弱性スキャナデータを取り込む場合、Scannerを先に選択する）

その他のオプション設定を定義する、例えば収集頻度、メール通知、Live Data



Best Practice Checks

- コンフィグファイルの精査
  - ネットワーク機器メーカー、そして米国NIST機関が推奨するデバイスハードニング（強化）設定項目集
  - ～130事項が搭載され、コンフィグファイルが取り込まれる度に稼働する
  - 必要に応じてチェック項目を外す事も出来る
  - カスタマイズで組織特有のチェックも構築が可能
  - Best Practice Checksはトポロジーマップを整えなくても機能するのですぐに成果を上げる事が出来る

Best Practice Checks

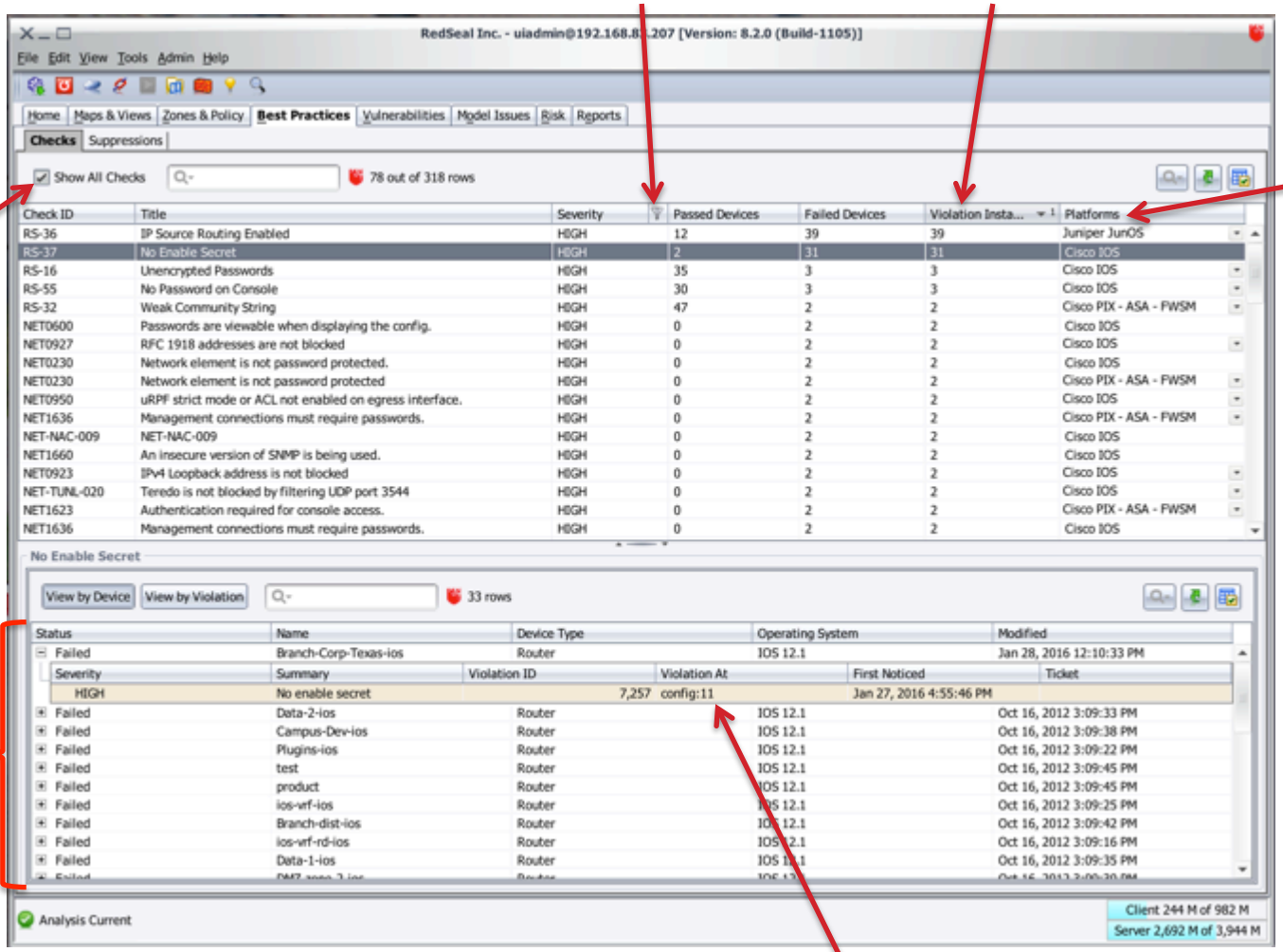
フィルタリングが可能

警告の数でソーティング

該当する機種・OS

このチェックを外すとモデルに当該するチェックだけが表示される

チェック項目の詳細



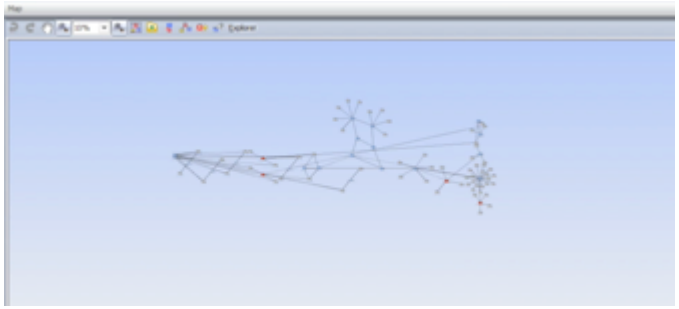
（行数が表示されていると）
右クリック｜Show in Config Fileで
コンフィグ内で確認

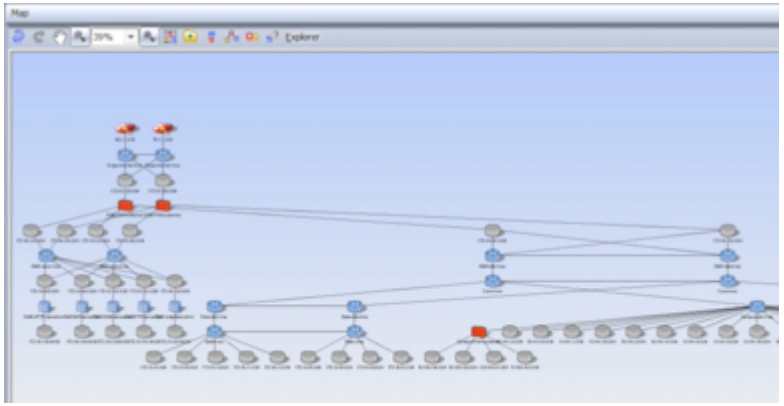
Topology Layout

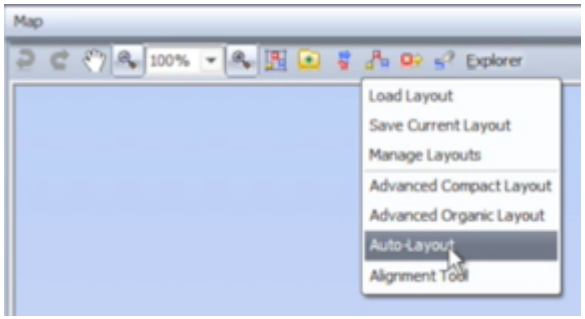
- トポロジーマップの生成
  - RedSealはインターフェース定義を基に物理的な繋がりを可視化する
  - オプションで動的ルーティングを重視させる事もできるが、コンフィグファイル収集の際にLive Dataを定義する事が必要
    - Live Dataは実機アクセスでしか収集出来ない
- グループの定義とネットワーク構成図の作成
  - 例：Internet、DMZ、Border、Campus、Critical Servers、等
  - 既存のネットワークマップ資料（例えばVisioやパワーポイント）を基に概ねのグループ構成を構築する
  - グループの色を変えてトポロジーマップを分かり易くする
    - 例：Internetは赤、DMZは紫、Critical Serverは黄色、等

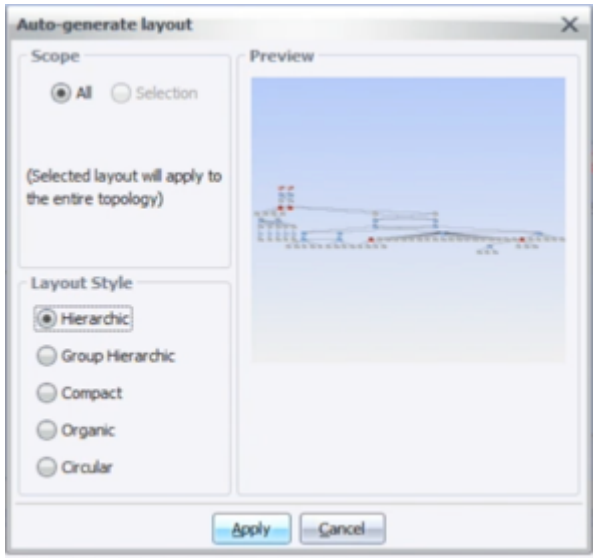
Topology Layout

- Auto-Layout ツールを使い、グループの作成作業を開始する



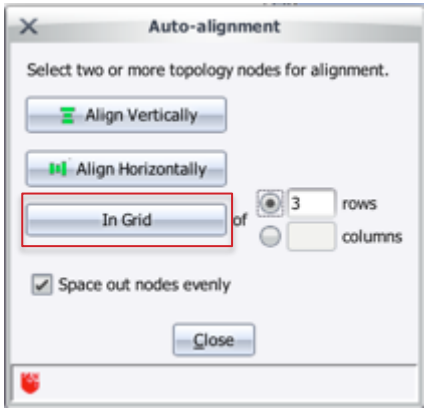


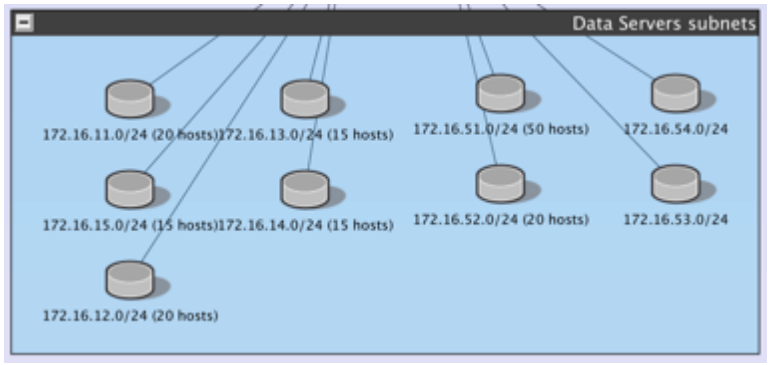


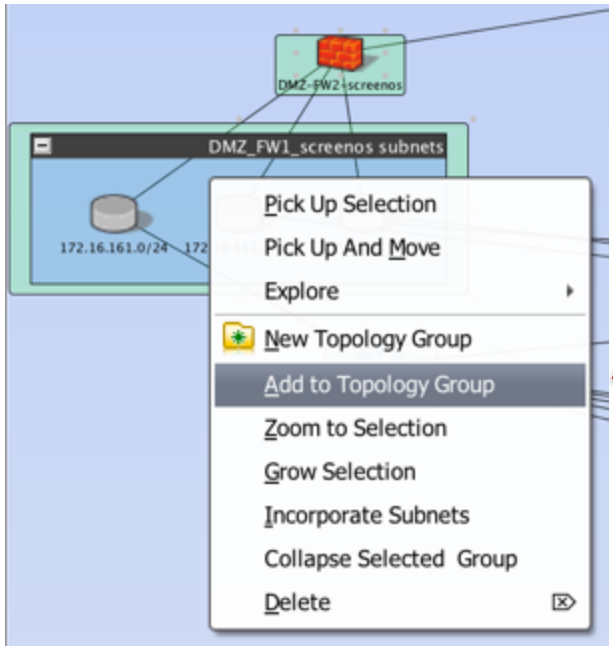


Topology Layout

- デバイスの役割、地域、ネットワークセグメント等によってデバイスとサブネットをグループに入れ、配置する
- Alignment Tool を使うと素早くオブジェクトをきれいに並べる事が出来る

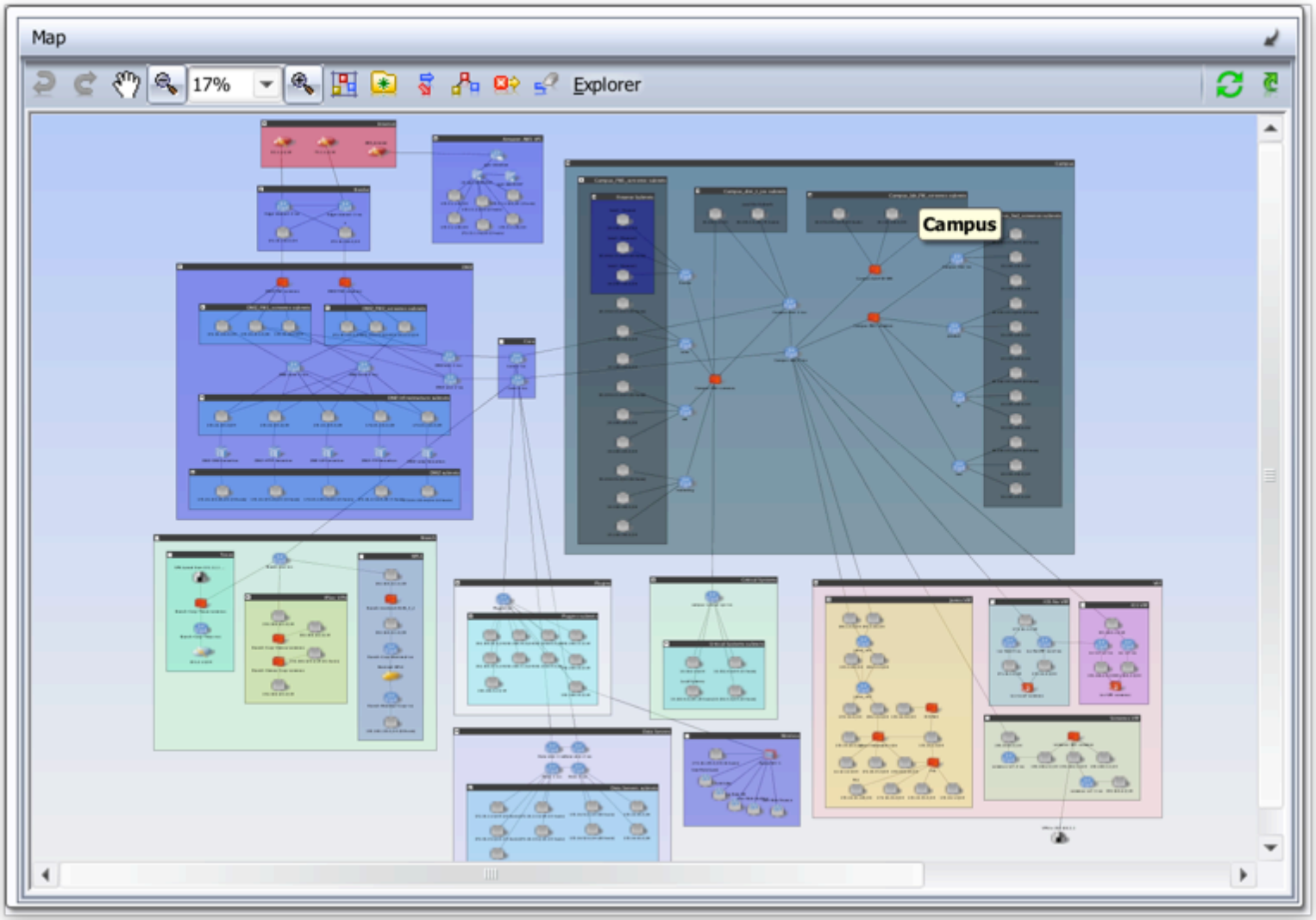






選択されたオブジェクトを
トポロジーグループに追加
（又は新規グループを作成）

Topology Map 完成例



Model Issues

- RedSeal モデルの整合性を確認する機能
  - モデルが正確でないと、あらゆる機能が誤った結果を出す可能性がある
    - 例えば、地球の反対側にあるデバイスとローカルのデバイスに同じIP Addressが定義されていた場合、サブネットを切断（Edit | Split Subnet）をする必要がある
- Model Issuesは19項目あるが（2016年6月現在）最低限次のModel Issueを解消する事を推奨する
  - MI-1 – Overlapping Subnets
  - MI-3 – Colliding IP Addresses
- MI-1 と MI-3 の対処方は次のページで解説

MI-1: Overlapping Subnets

- モデル内にサブネットが被っている事を表す

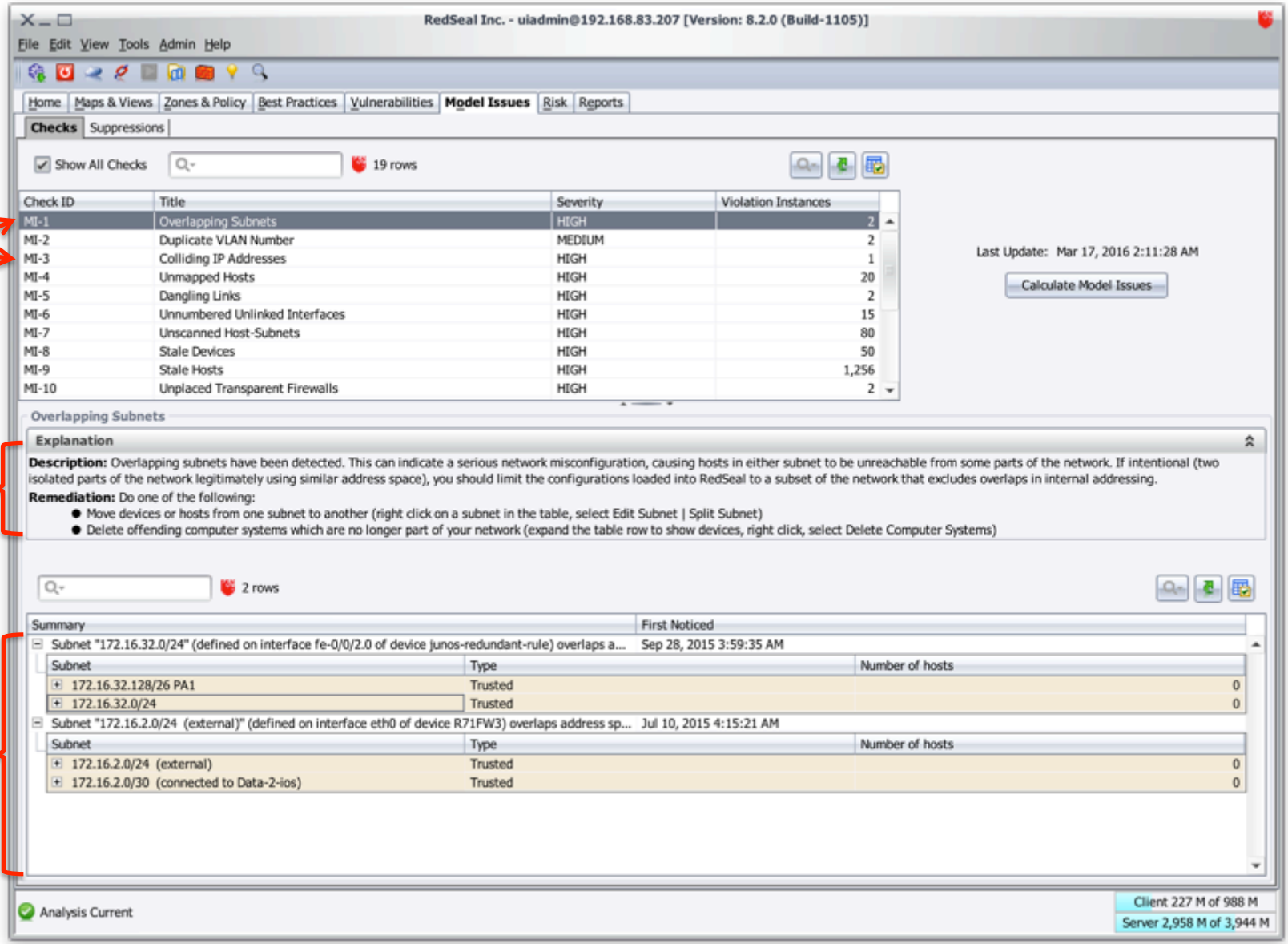
- 物理的に同じ場所に存在しないデバイスが重なるIP Addressサブネットが定義されている場合等が考えられるが、設定ミスの可能性もあり得る
  - その他に、古い設定ファイル等が取り込まれた場合
- 対処方
  - 物理的に離れている場合
    - エントリーを選択し、右クリックメニューからEdit Subnet | Split Subnetを選択し、サブネットを分ける
  - 設定ミス
    - ミスを訂正し、更新されたコンフィグファイルを取り込む
  - 古い設定ファイル
    - 最新の設定ファイルを取得し取り込むか、古い設定ファイルから可視化されたデバイスをモデルから削除する

MI-3: Colliding IP Addresses

- モデル内にIP Addressが被っている事を表す

- 理由・対処方はMI-1: Overlapping Subnetsと同様、以下の通り:
- 物理的に同じ場所に存在しないデバイスが重なるIP Addressが定義されている場合等が考えられるが、設定ミスの可能性もあり得る
  - 設定ミスの場合、ネットワークに支障が起こっている可能性が大
  - その他に、古い設定ファイル等が取り込まれた場合
- 対処方
  - 物理的に離れている場合
    - エントリーを選択し、右クリックメニューからEdit Subnet | Split Subnetを選択し、サブネットを分ける
  - 設定ミス
    - ミスを訂正し、更新されたコンフィグファイルを取り込む
  - 古い設定ファイル
    - 最新の設定ファイルを取得し取り込むか、古い設定ファイルから可視化されたデバイスをモデルから削除する

Model Issues



最低限この二つの
MIを解決する

Model Issueの
詳細と解決案

Model Issueの詳細:
ここからEdit Subnet

Threat Sources

- RedSealには概ね2種類のサブネットタイプがある
  - UnTrusted
    - 信頼性の低いサブネット
    - Internet、Extranet、Local UnTrustedの3種類がある
      - Local UnTrustedは組織内に依存するが、何らかの理由で信頼性が低いと判断されたサブネット
        - 例えばゲストワイアレスセグメント
  - Trusted
    - 組織に依存するサブネット
    - 安全を確認したいサブネット

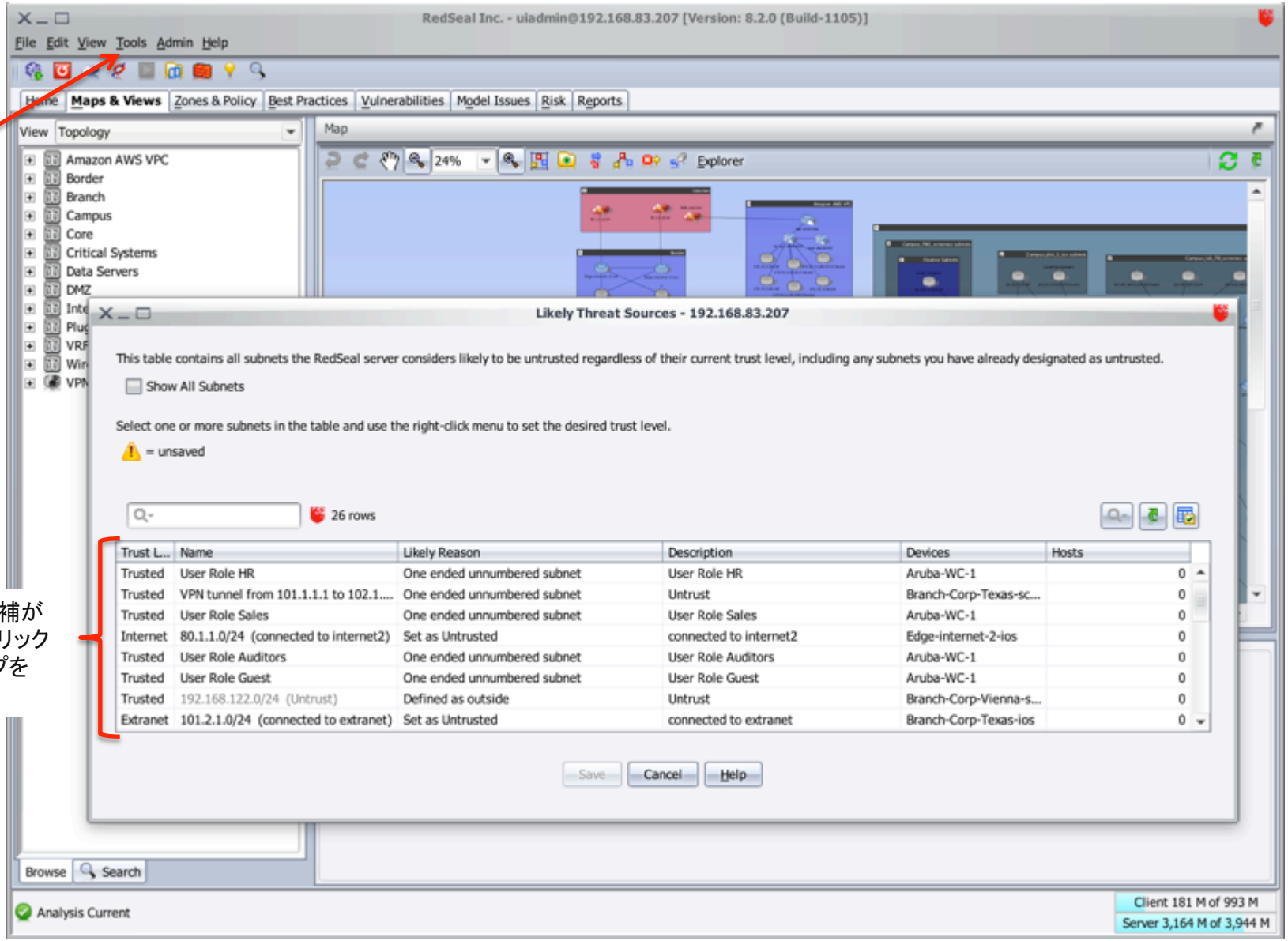
- RedSealは主にUnTrustedからTrustedへのアクセスと脅威を分析する

- **重要事項:** 初期導入時にUnTrustedを定義する必要がある

Threat Sources

Toolsメニューから
Threat Sources を
選択

UnTrustedの候補が
表示され、右クリック
メニューでタイプを
定義出来る



Analysis

- RedSealは新たなデバイス、またはスキャナデータ等が取り込まれる度にAnalysis（即ち分析）をする必要があります
- 自動コンフィグ収集が設定されると、データコレクションタスクが稼働する度にAnalysisが自動的に実行される
- 手動でAnalysisを実行するにはHomeタブ画面からAnalyzeボタンを叩く

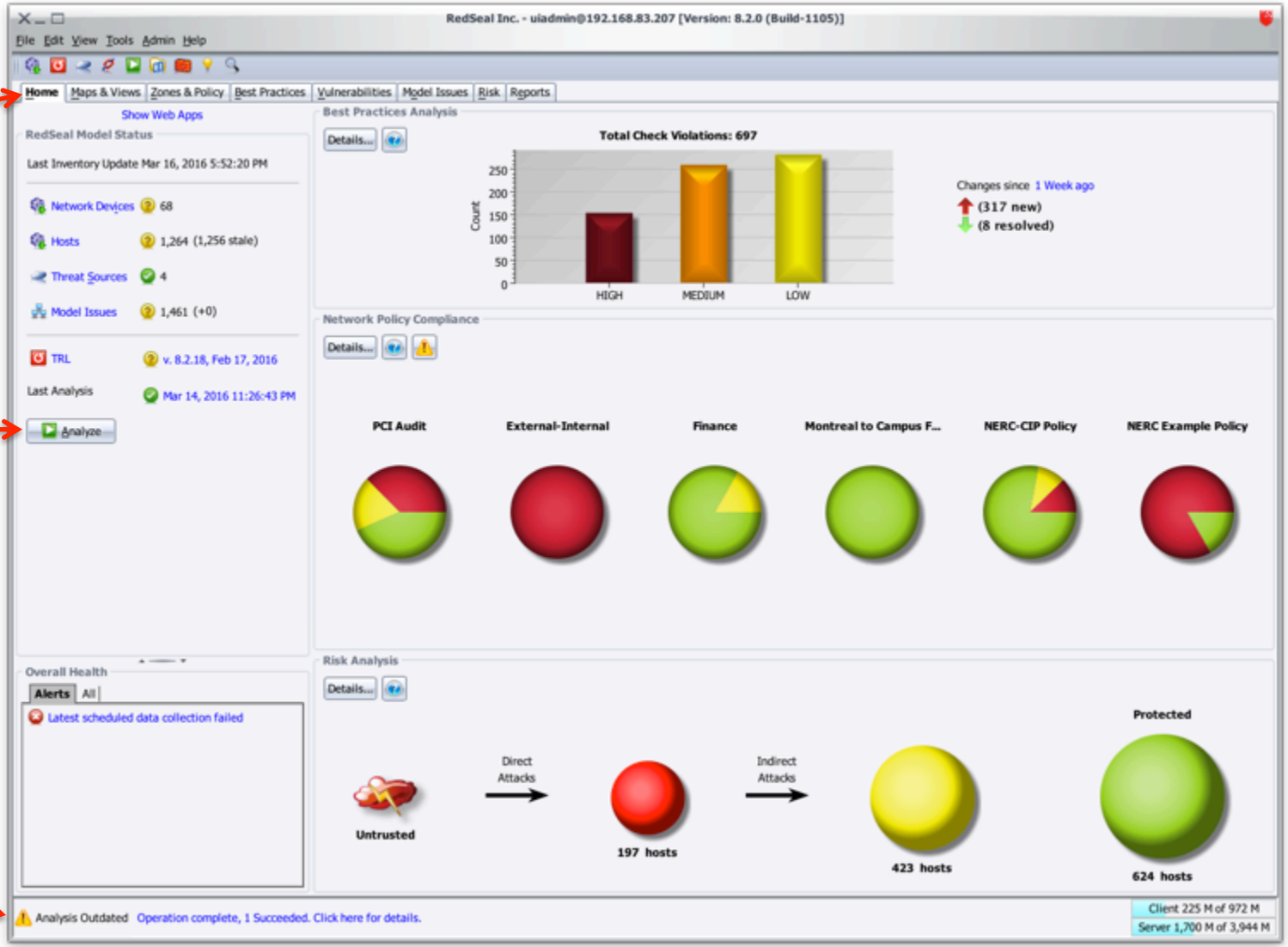
- Analysisの所要時間はモデルの規模の大きさ、そして個々のデバイス設定の複雑さにより影響される
  - 例えば、同じルータでもインターフェースの定義が5つ対100あると、後者のルータの分析時間の方が長くかかる
  - ファイアウォールルールの数や脆弱性スキャナのデータの大きさ等も影響を及ぼす
  - 以上の理由の為、RedSealサーバーの動作環境の推奨は難しい

Analysis

AnalysisはHome画面から実行可能

Analyzeボタンはモデルが変わる度に（例：デバイスが追加・削除される、等）クリック可能になる

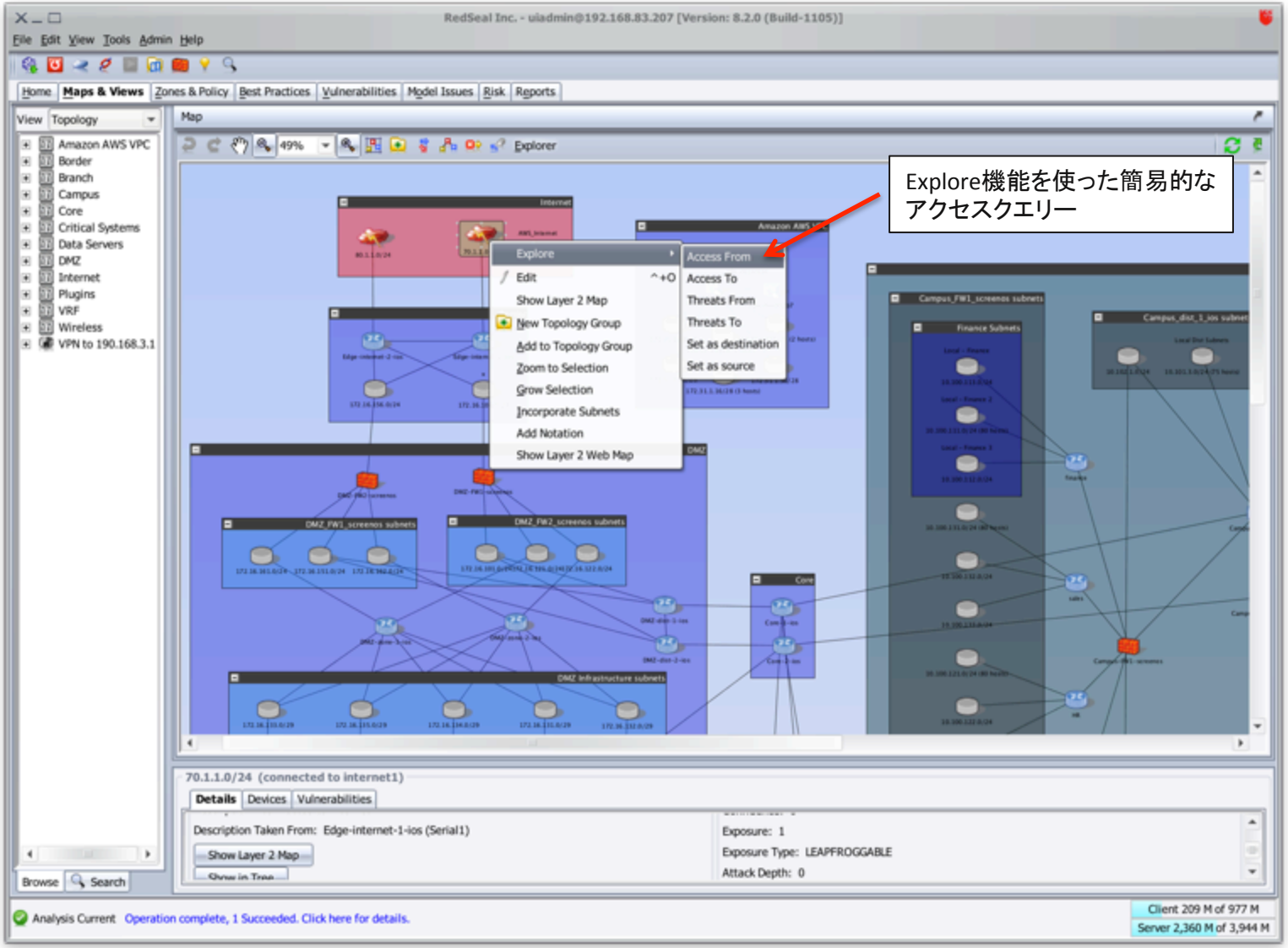
Analysisが必要な場合、ウィンドウ下部にメッセージが表示される



Access Queries

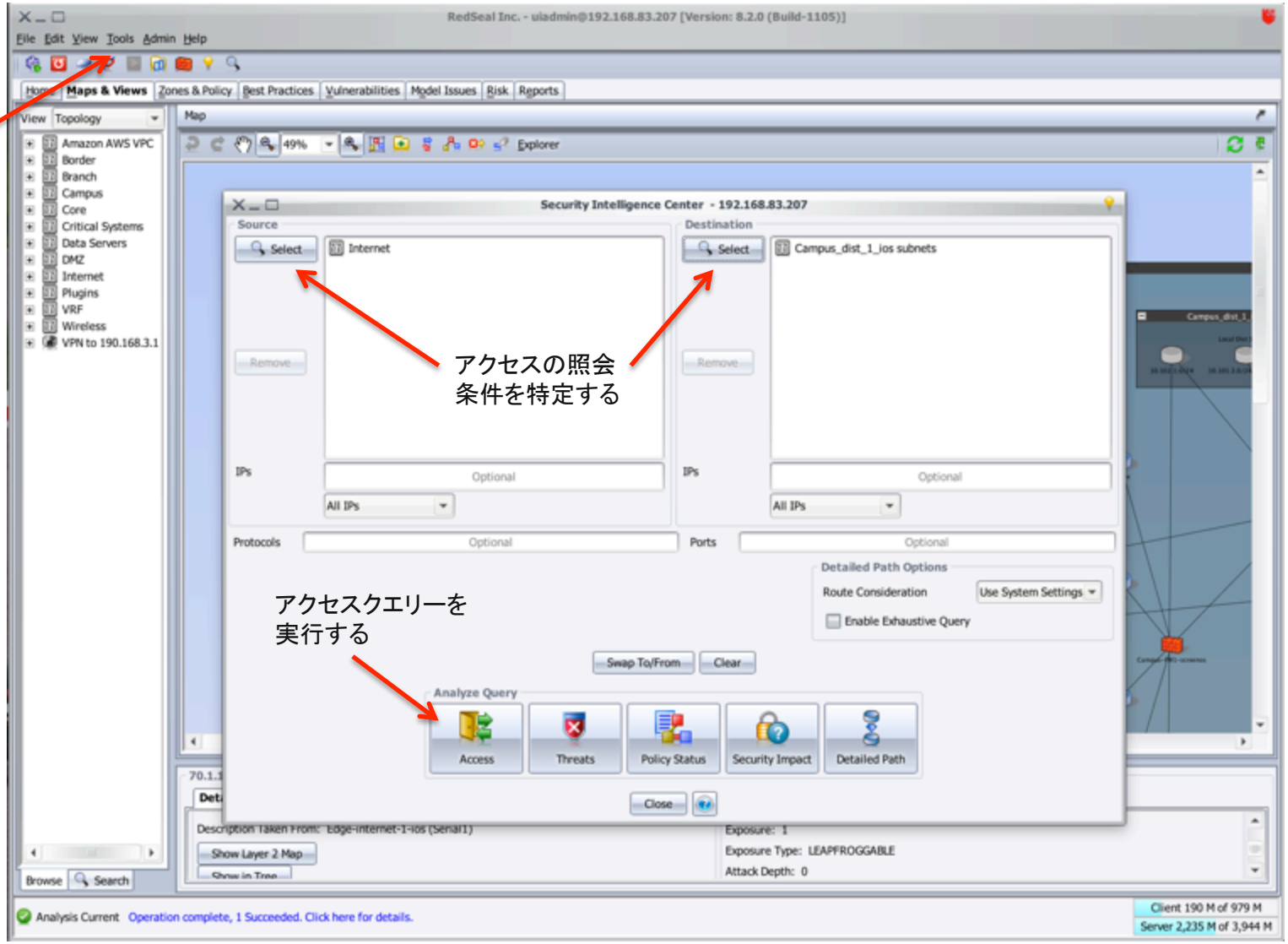
- Access Queriesはアクセスパスの照会機能
- クエリーは複数のやり方がある
  - Maps & Views画面にてマウスを使って操作する
    - サブネットを選択し、右クリックメニューから”Access From”、または“Access To”を実行する
  - Tools | Security Intelligence Center を開き、特定のSourceとDestination（オプションでProtocolとPortも）を選択し、“Access”を実行する
  - Tools | Security Query Manager を開き、クエリーを構築する
- 一般的なクエリーの操作法は簡易的に実施できるMaps & Viewsからのマウス操作
- 調査や更新管理などによく用いられる操作法はSecurity Intelligence Manager
- レポート出力の為のクエリーはSecurity Query Managerが最適

Access Queries – 簡易的なクエリー



Access Queries – 検証や調査等の場合

Toolsメニューから
Security Intelligence
Centerを選択

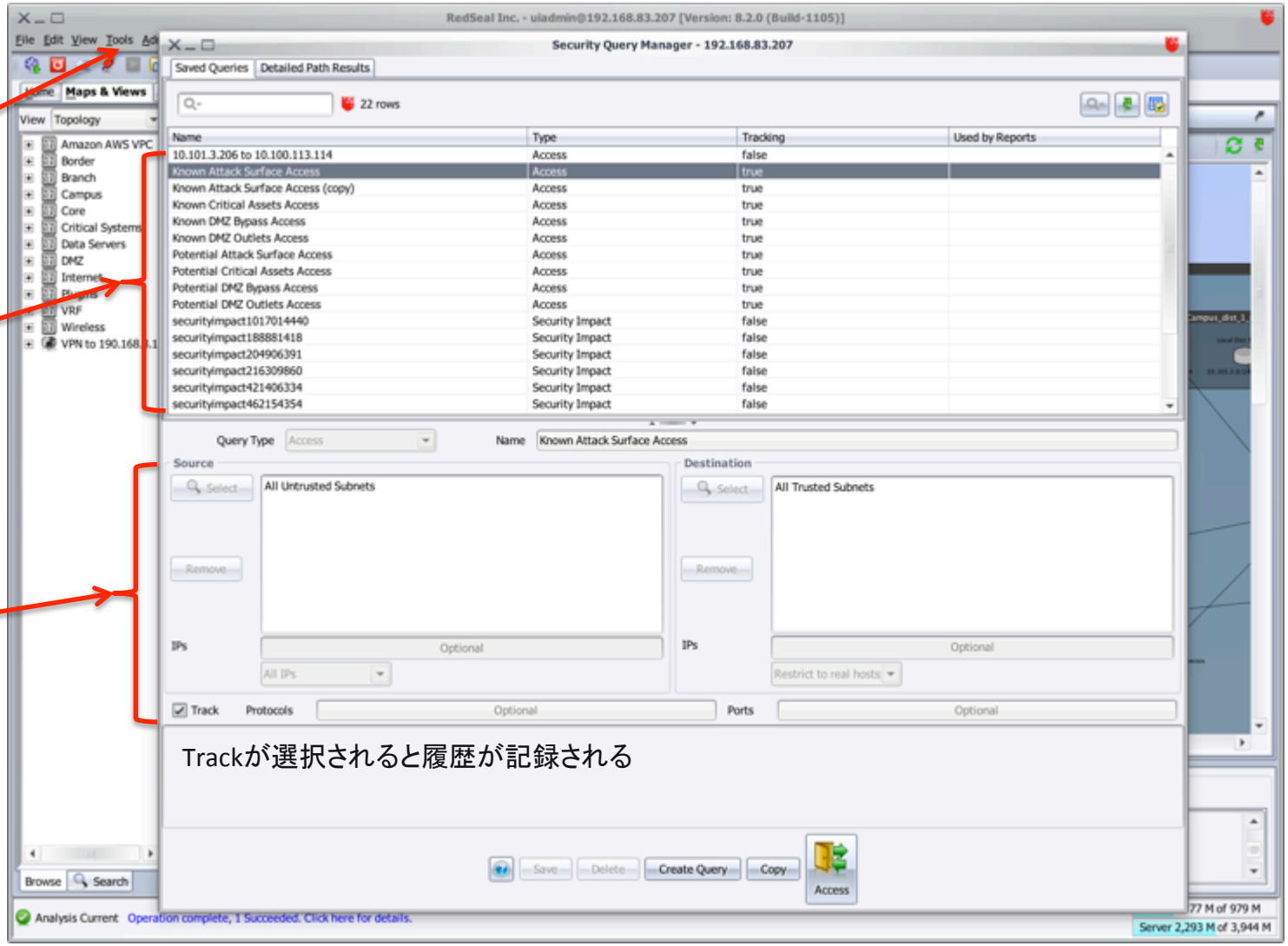


Access Queries – レポート出力の為のクエリー構築

Toolsメニューから
Security Query
Managerを選択

ビルトインで搭載
されたクエリーの
他に今までに実施
されたクエリーも
含む

新たなクエリーを
構築する

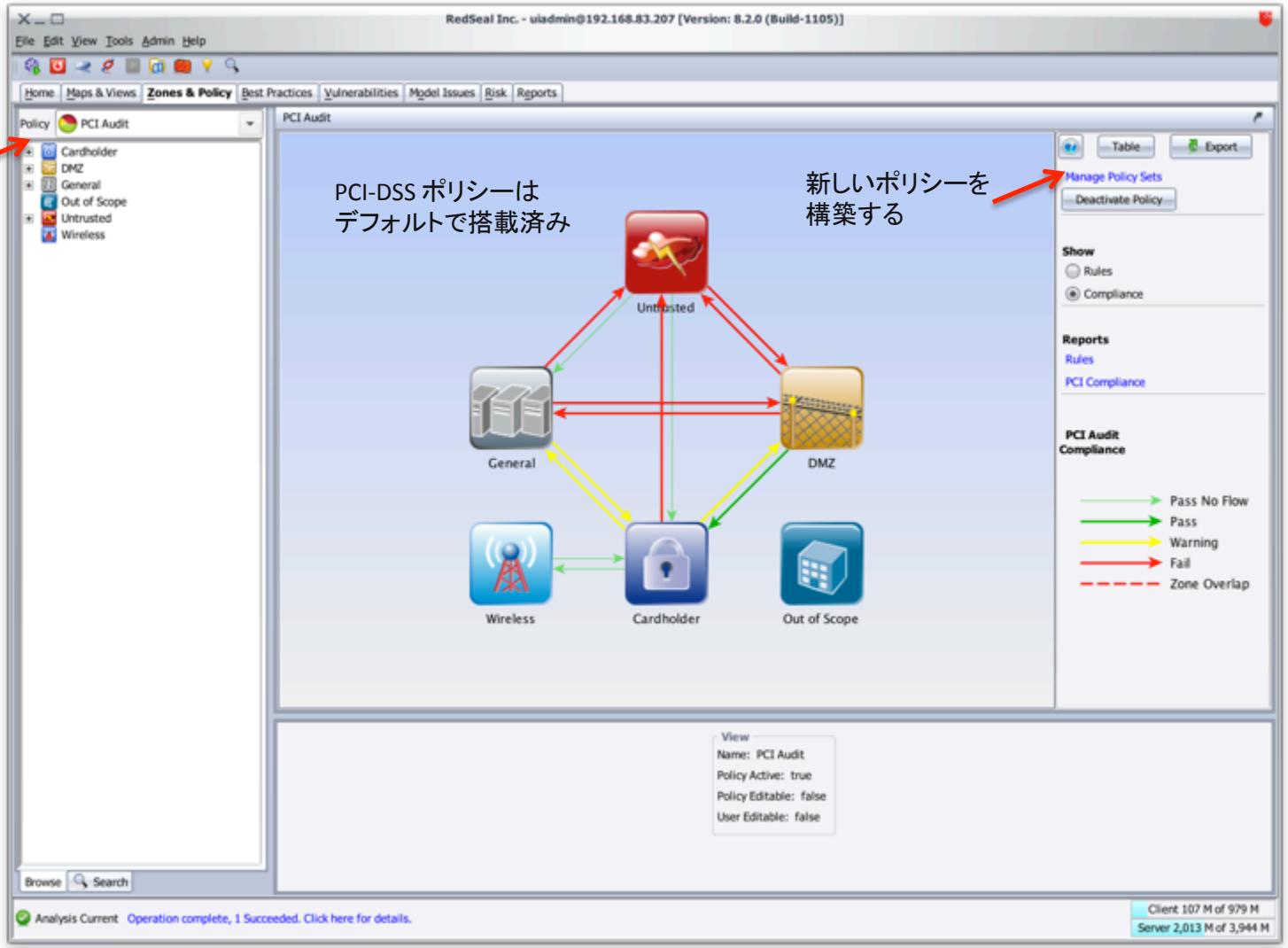


Security Segmentation (Zones & Policy)

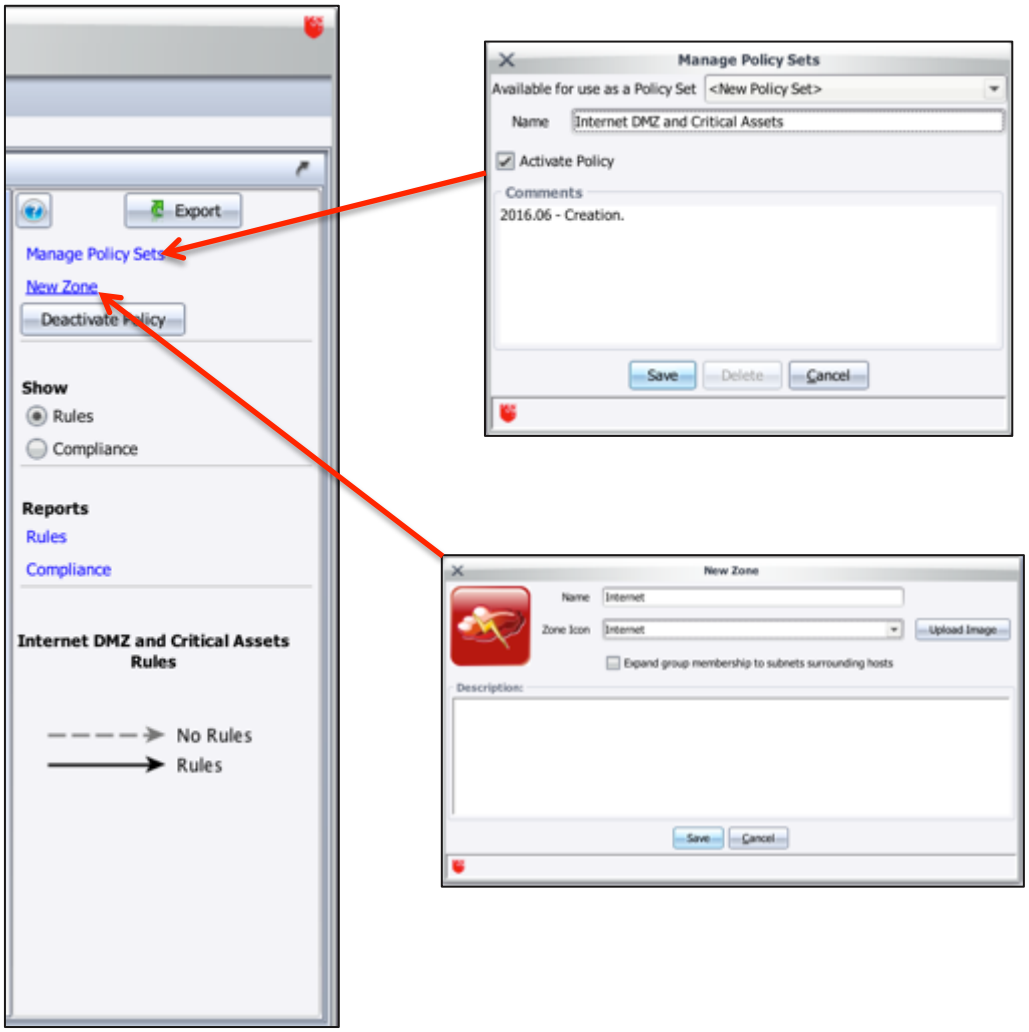
- Zones & Policyはセグメンテーションの確認をする為に便利な機能
- 機械化のおかげで人力では確認しきれない領域まで随時確認が可能
- 想定外のアクセスや意図しないアクセスを発見できる
- 米国ではPCI-DSSやNERC-CIP等の法令規制の遵守の為によく使われる

Security Segmentation (Zones & Policy)

ドロップダウンから
ポリシーを選択



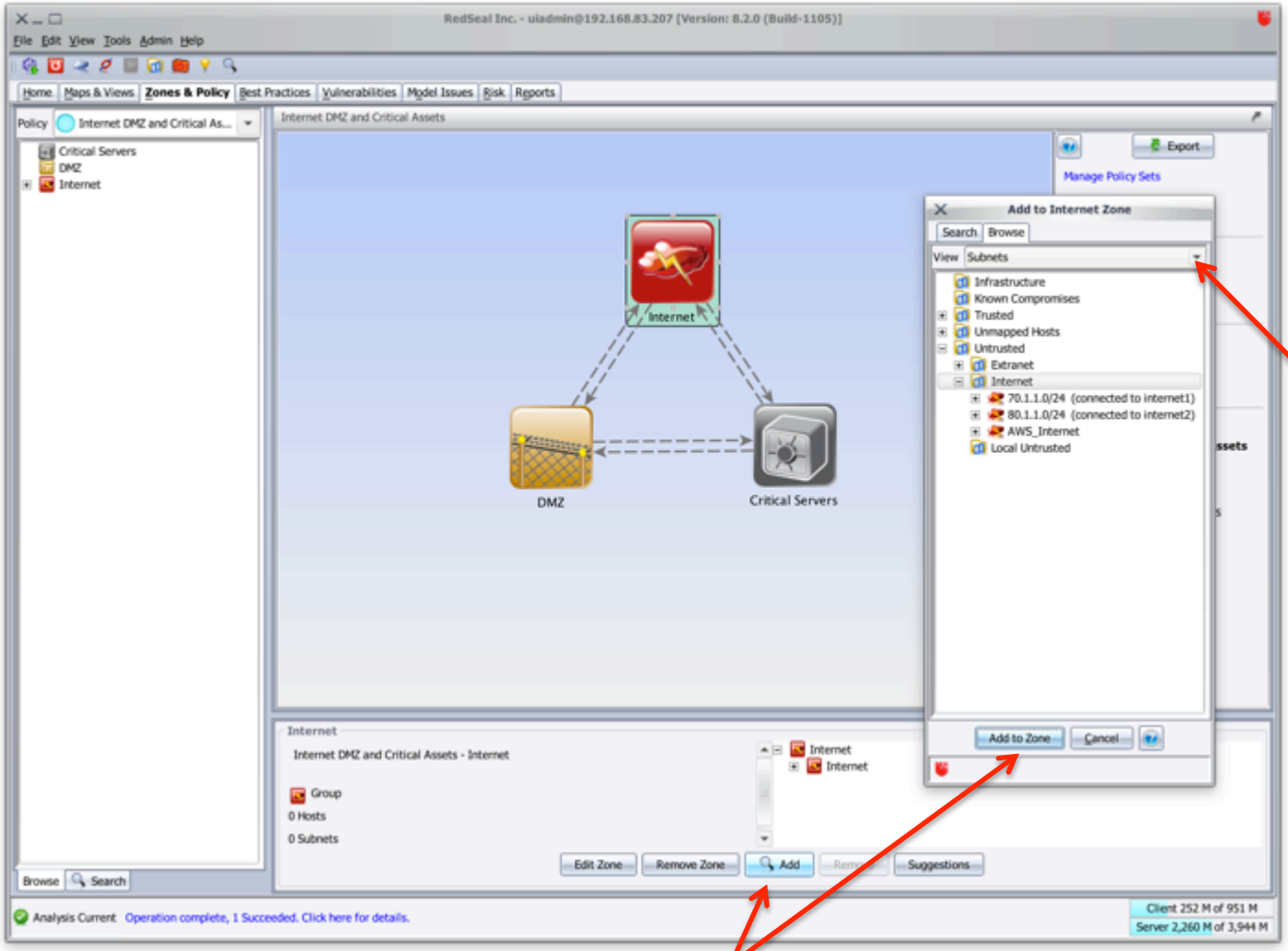
Security Segmentation (Zones & Policy)



Manage Policy Setsから
新規ポリシーを構築

New Zoneからセグメンテーションを
確認したいネットワークセグメントの
オブジェクト(“Zone”と呼ぶ)を必要
な数だけ作る

Security Segmentation (Zones & Policy)



Search、Browse、そしてViewのドロップダウンを使い分け、該当するサブネットを見つけ出し、Add to Zoneをする

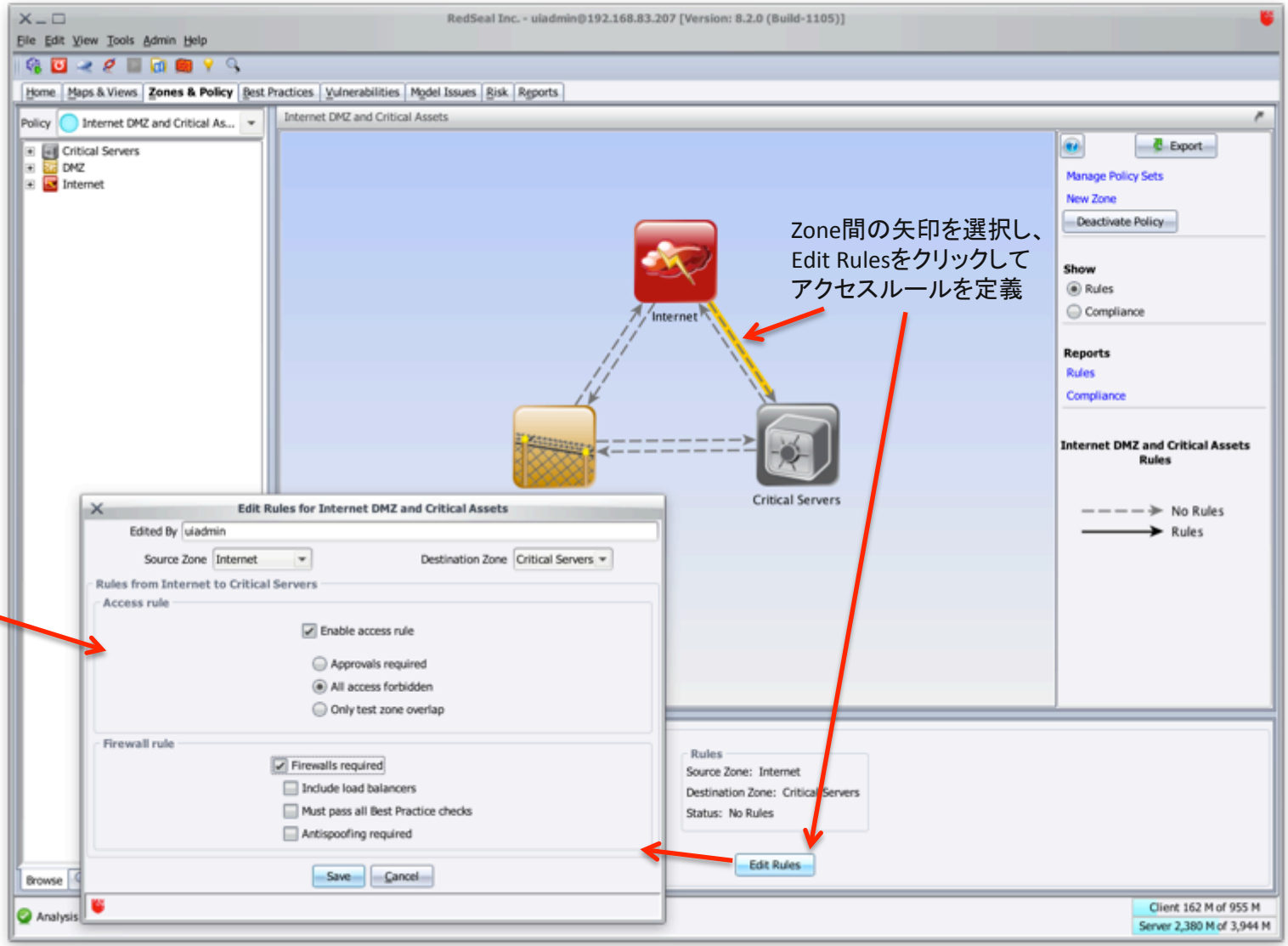
Zoneが構築された次に、該当するサブネットを追加

Security Segmentation (Zones & Policy)

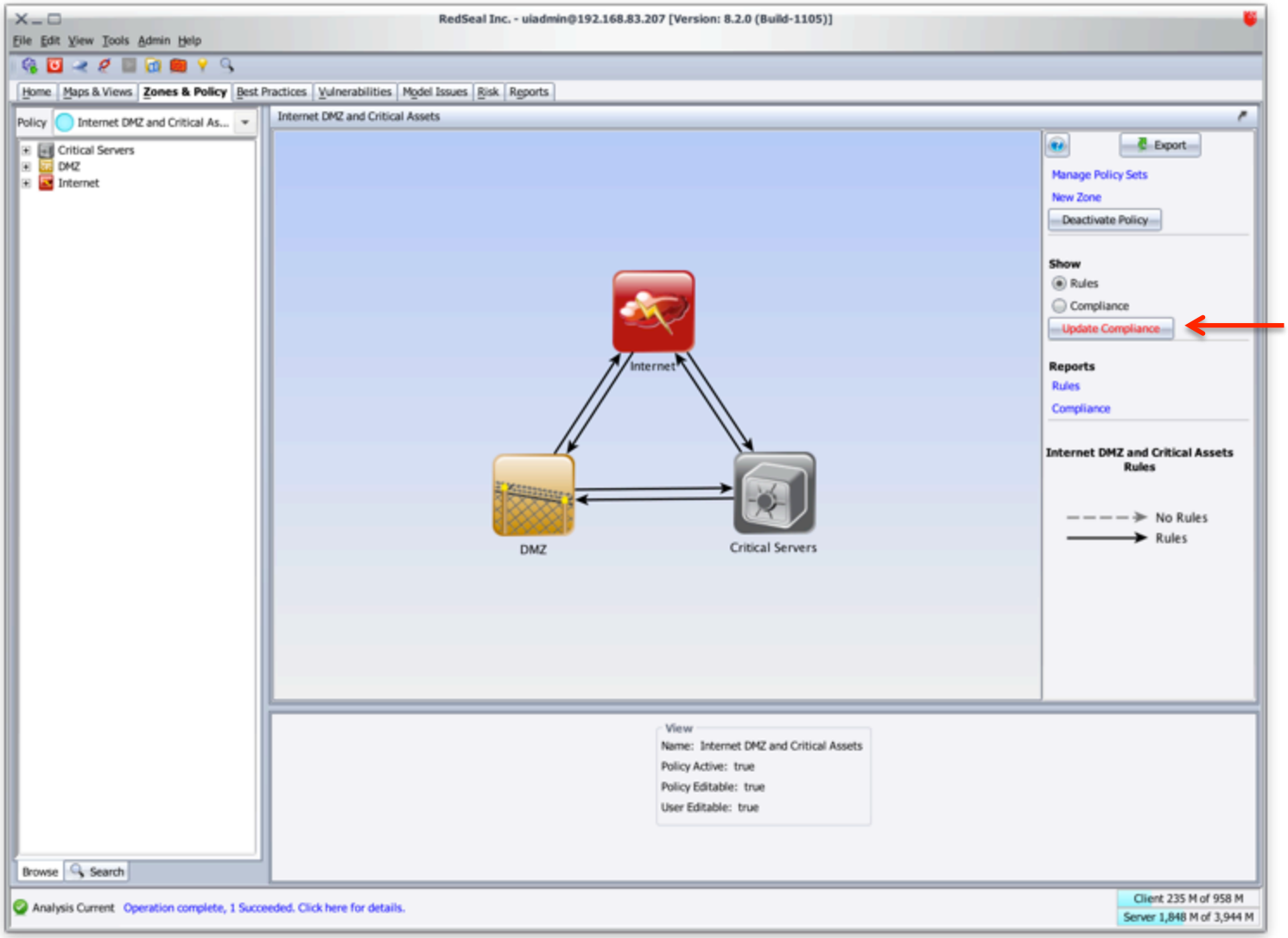
Approvals required:
- 認証必要

All Access Forbidden:
- アクセス禁止

Only test zone overlap:
- Zoneが被っているか確認



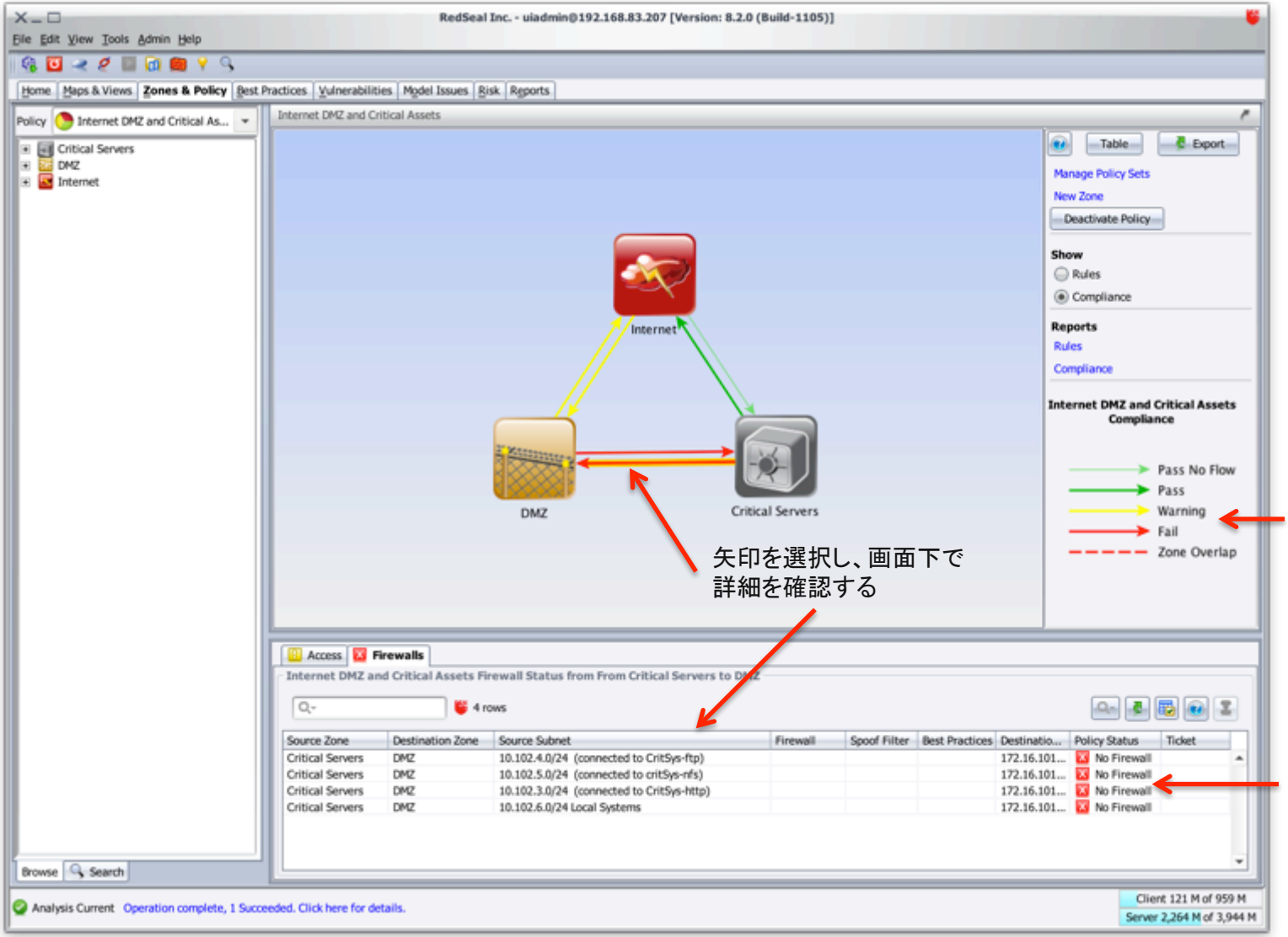
Security Segmentation (Zones & Policy)



アクセスルールの定義を終えるとUpdate Complianceボタンを叩き、Compliance画面で結果が確認できる

Zones & PolicyはAnalysisが実施される度に更新される

Security Segmentation (Zones & Policy)



セグメンテション確認の
結果が色別で表示される

ここからDetailed Pathの
クエリーを実施して確認
作業が行える

トラブルチケットの発生も
可能

Vulnerability Management

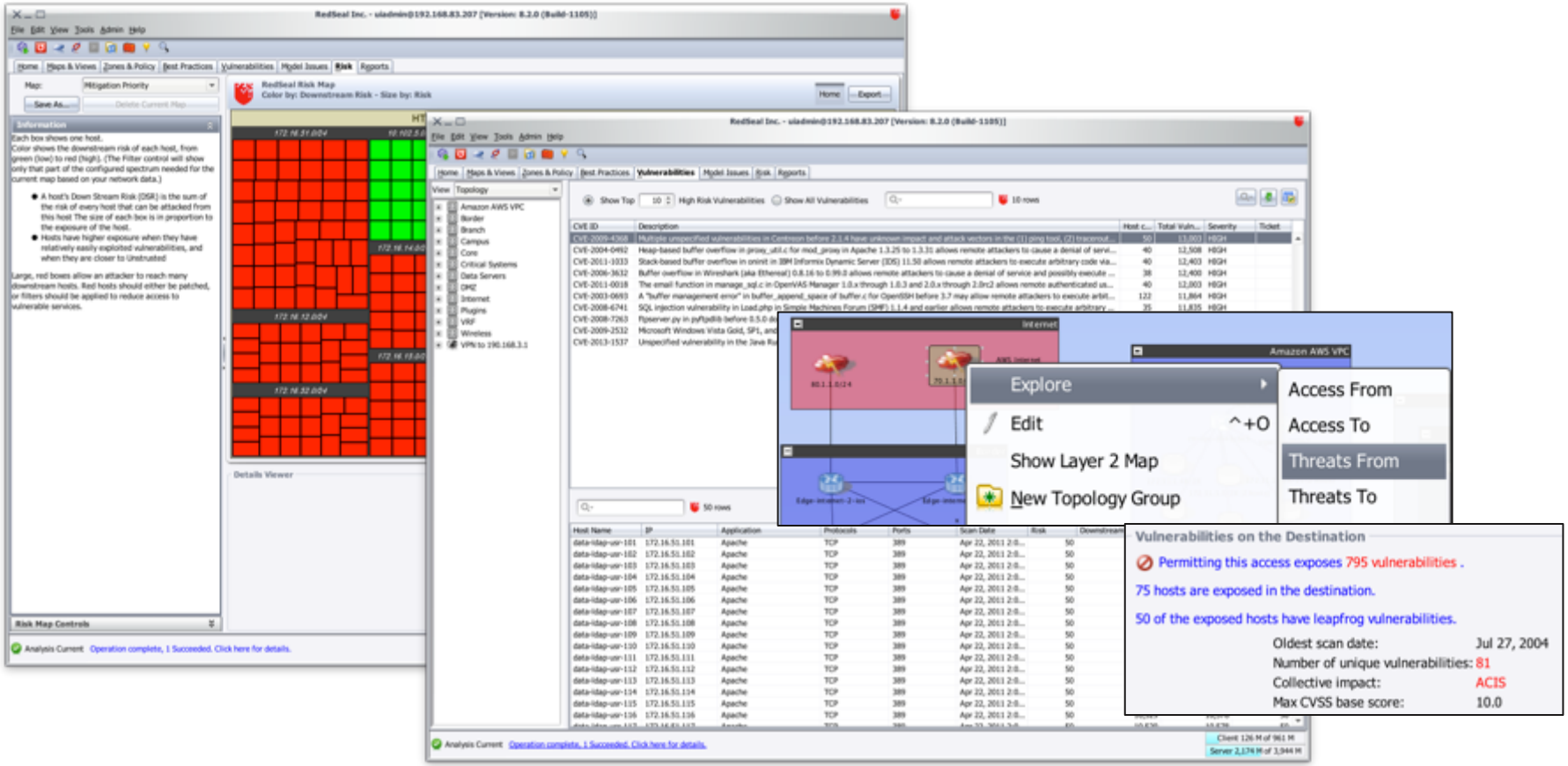
- Vulnerability Management（脆弱性の管理）に関連する機能を実装する為には まず初めに他社脆弱性スキャナ製品から出力されたデータが必要
- 対応する脆弱性スキャナ（2016年6月現在）

MANUFACTURER	DEVICE NAME/OS	VERSIONS SUPPORTED
Alert Logic (Critical Watch)	FusionVM	4
DDI	Frontline	5.0
BeyondTrust	REM Security Management Console	3.7.9 & 3.8
BeyondTrust	eEye Retina	3.8 & 5.16
McAfee	Vulnerability Manager	7.0.1 & 7.5
Outpost24	OUTSCAN, HIAB (hacker-in-a-box)	3.2.7
Open source	nMap	6.25
Qualys	QualysGuard	7.6
Rapid7	NeXpose	4.12
Symantec	Vulnerability Manager	10.0.5
Tenable	Nessus	4.6.2.1 & 4.8, 6.0
Tripwire (nCircle)	IP360	6.8.9, 6.9, & 7.3.x

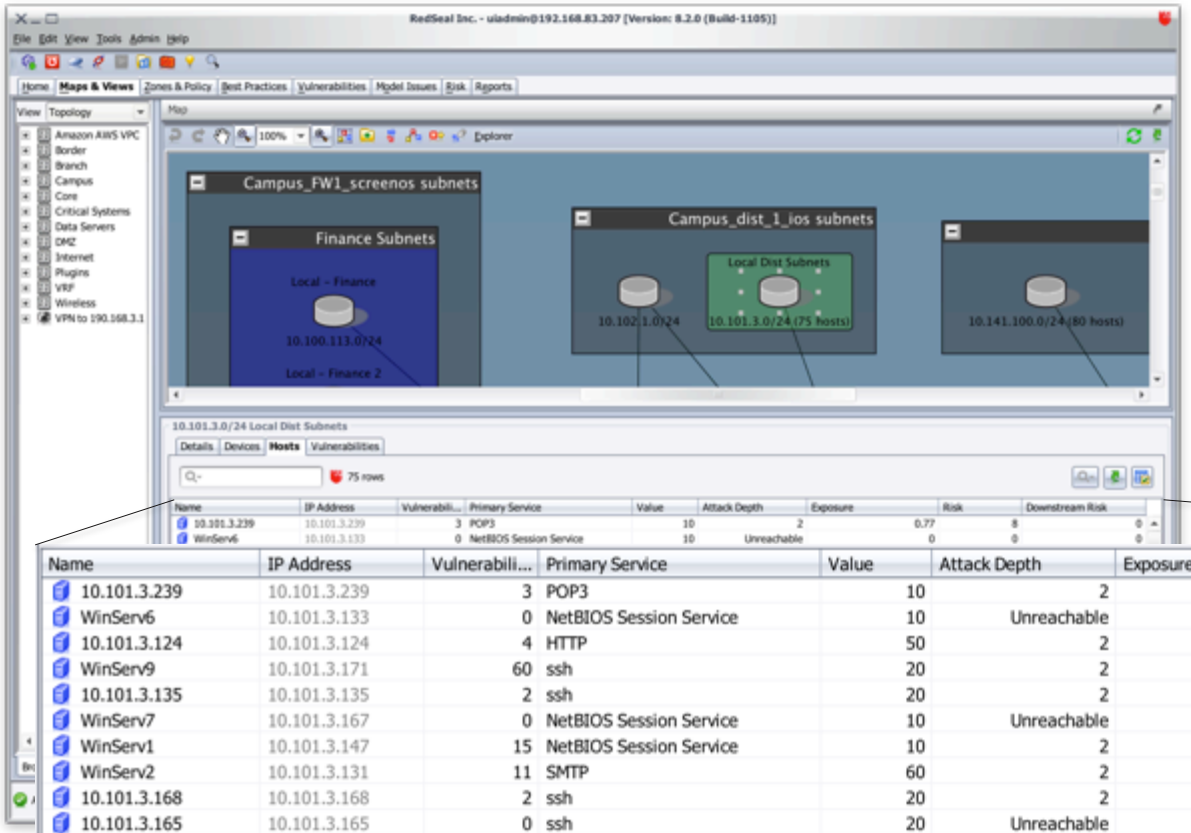
- スキャナデータはData Collection機能を経由して取り込みが可能
  - 各スキャナ製品データの取り込みに関しての詳細は *RedSeal Data Import Plug-ins Guide*を参照

Vulnerability Management

- スキャナデータを取り込むと主にVulnerabilitiesとRisk画面に情報が反映
- Maps & Views内では“Threats From/To”が実装
- Security Intelligence Centerにては脆弱性の情報がアクセスに反映される



Vulnerability Management



Name	IP Address	Vulnerabili...	Primary Service	Value	Attack Depth	Exposure	Risk	Downstream Risk
10.101.3.239	10.101.3.239	3	POP3	10	2	0.77	8	0
WinServ6	10.101.3.133	0	NetBIOS Session Service	10	Unreachable	0	0	0
10.101.3.124	10.101.3.124	4	HTTP	50	2	0.74	37	0
WinServ9	10.101.3.171	60	ssh	20	2	0.98	20	0
10.101.3.135	10.101.3.135	2	ssh	20	2	0.98	20	0
WinServ7	10.101.3.167	0	NetBIOS Session Service	10	Unreachable	0	0	0
WinServ1	10.101.3.147	15	NetBIOS Session Service	10	2	0.93	9	0
WinServ2	10.101.3.131	11	SMTP	60	2	0.93	56	0
10.101.3.168	10.101.3.168	2	ssh	20	2	0.98	20	0
10.101.3.165	10.101.3.165	0	ssh	20	Unreachable	0	0	0
10.101.3.206	10.101.3.206	3	ssh	20	1	0.99	20	10,529
WinServ7	10.101.3.134	0	NetBIOS Session Service	10	Unreachable	0	0	0
WinServ8	10.101.3.136	0	ssh	20	Unreachable	0	0	0
10.101.3.145	10.101.3.145	9	ssh	20	2	0.98	20	0
WinServ5	10.101.3.230	11	NetBIOS Session Service	10	2	0.74	7	0
WinServ9	10.101.3.208	60	ssh	20	2	0.98	20	0

脆弱性スキャナから取り込まれたデータを基にあらゆるメトリクスが表示、及び分析される

サブネットを選択してHosts画面を選択すると詳細が表に表せられる

Vulnerability Prioritization

- Name: ホストネーム
- IP Address: IP アドレス
- Vulnerability: (ホストが持つ)脆弱性の数
- Primary Service: 主要サービス
- Value: ホストの価値
- Attack Depth: “攻撃深度”
  - 1:直接攻撃可能
  - 2:間接攻撃可能
  - Unreachable: UnTrustから攻撃不可能
- Exposure: CVSS Base ScoreとAttack Depthを踏まえた“露出度”
- Risk: ValueとExposureを掛け合わせた結果の数値
- Downstream Risk: このホストが攻略されて踏み台攻撃等で2次攻撃が展開されたと仮定した場合、攻撃可能なサブネットに依存するホスト全てのRiskスコアを合算した数値

Name	IP Address	Vulnerabili...	Primary Service	Value	Attack Depth	Exposure	Risk	Downstream Risk
10.101.3.239	10.101.3.239	3	POP3	10	2	0.77	8	0
WinServ6	10.101.3.133	0	NetBIOS Session Service	10	Unreachable	0	0	0
10.101.3.124	10.101.3.124	4	HTTP	50	2	0.74	37	0
WinServ9	10.101.3.171	60	ssh	20	2	0.98	20	0
10.101.3.135	10.101.3.135	2	ssh	20	2	0.98	20	0
WinServ7	10.101.3.167	0	NetBIOS Session Service	10	Unreachable	0	0	0
WinServ1	10.101.3.147	15	NetBIOS Session Service	10	2	0.93	9	0
WinServ2	10.101.3.131	11	SMTP	60	2	0.93	56	0
10.101.3.168	10.101.3.168	2	ssh	20	2	0.98	20	0
10.101.3.165	10.101.3.165	0	ssh	20	Unreachable	0	0	0
10.101.3.206	10.101.3.206	3	ssh	20	1	0.99	20	10,529
WinServ7	10.101.3.134	0	NetBIOS Session Service	10	Unreachable	0	0	0
WinServ8	10.101.3.136	0	ssh	20	Unreachable	0	0	0
10.101.3.145	10.101.3.145	9	ssh	20	2	0.98	20	0
WinServ5	10.101.3.230	11	NetBIOS Session Service	10	2	0.74	7	0
WinServ9	10.101.3.208	60	ssh	20	2	0.98	20	0

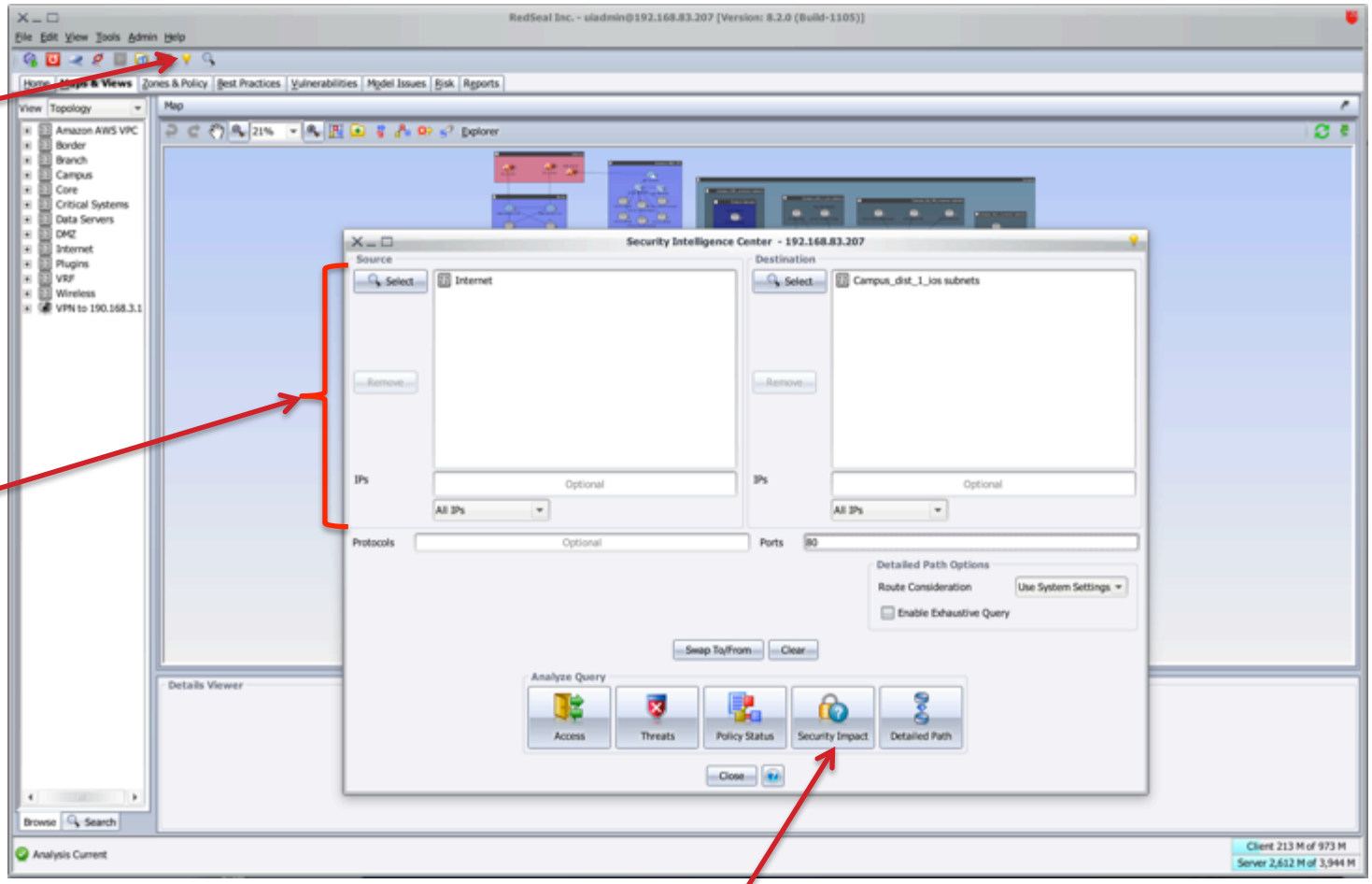
Security Intelligence Center – Security Impact Query

- Security Impact QueryはRedSealで可視化されたネットワークのセキュリティを確認する為の機能
- 主な機能はアクセスの有無、脆弱性の露出の可能性、そしてポリシーへの影響の確認
- 更新管理に大いに役たつ機能
  - ただし、コンフィグの定義の推奨、そして更新後の確認には使えない
- アクセスの有無
  - パスがOPENかBLOCKEDを表示する
  - Detailed Pathで繋がりを確認し、BLOCKEDの場合は何処でブロックされているのかが把握できる
  - パスがOPENだった場合、更新をする必要がないと判断出来る
- 脆弱性の露出
  - パスがOPENになった場合に露出される脆弱性の詳細を表示する
  - 踏み台攻撃の有無を表示する
  - 脆弱性スキャナのみでは不可能な動き
- ポリシーへの影響
  - 検証されているアクセスがセキュリティポリシーへどの様な影響を及ぼすのかを表示する
  - 色別でアクセスの認証が必要か、ポリシーに違反するアクセスなのかが一目瞭然
- Security Impact Queryを使うと、恐る恐る実施していた更新管理が自信を持って実施できる様になれる

Security Intelligence Center – Security Impact Query

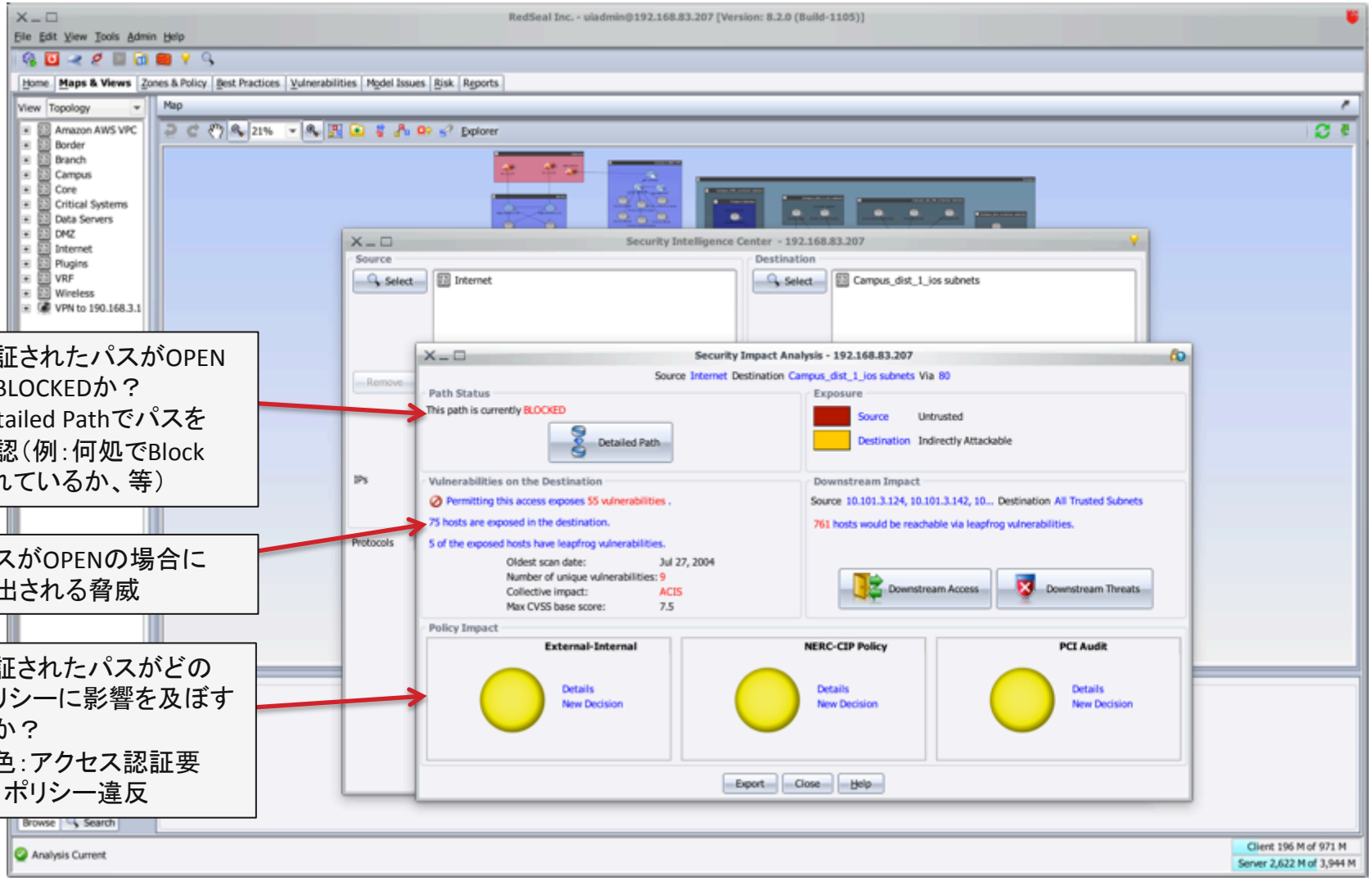
Toolsメニュー、又は電球ボタンを押し、Security Intelligence Centerを開く

SourceとDestinationの検証条件を選択・記入する

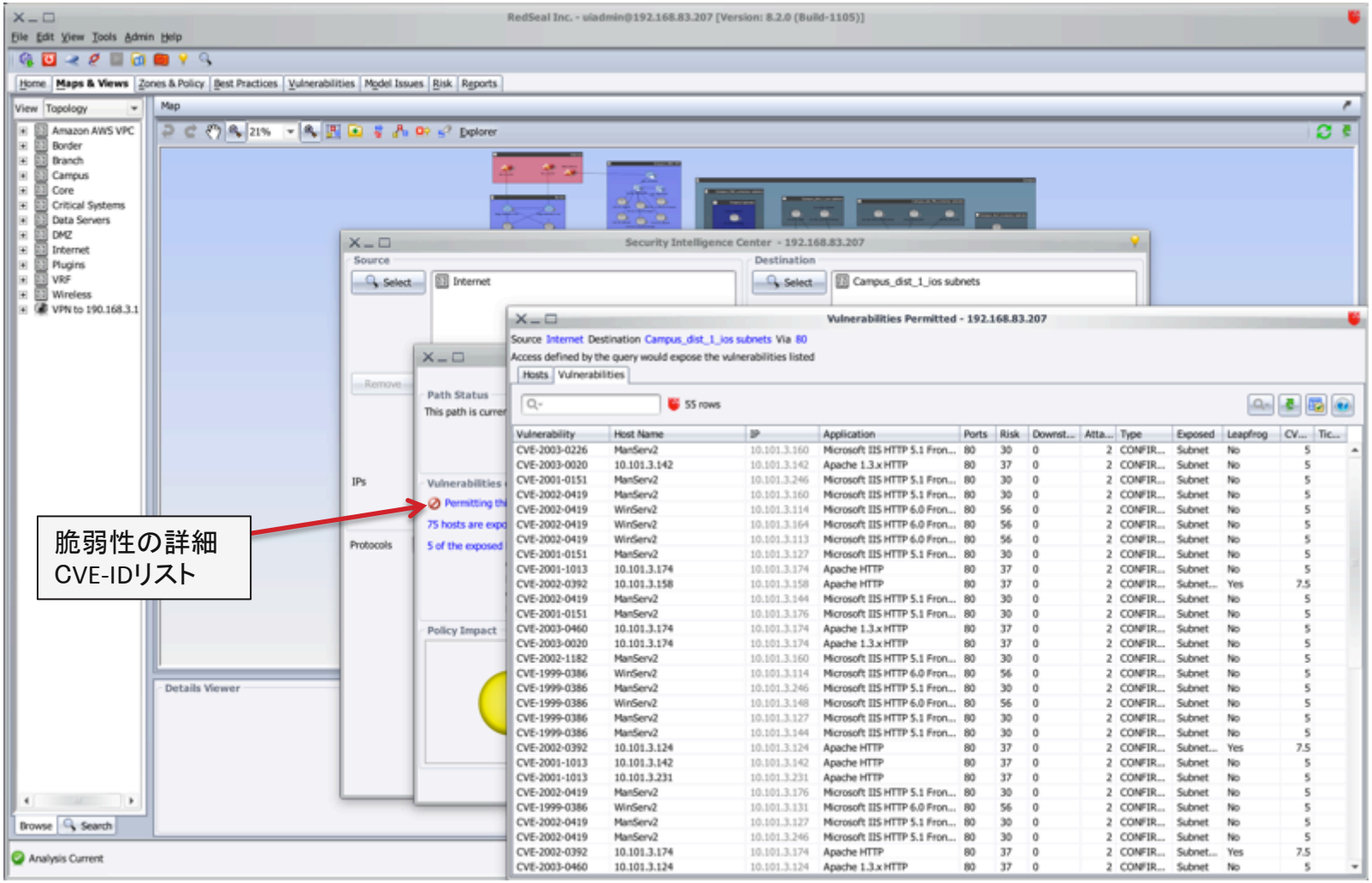


検証条件を記入した後、Security Impact Queryを実行する

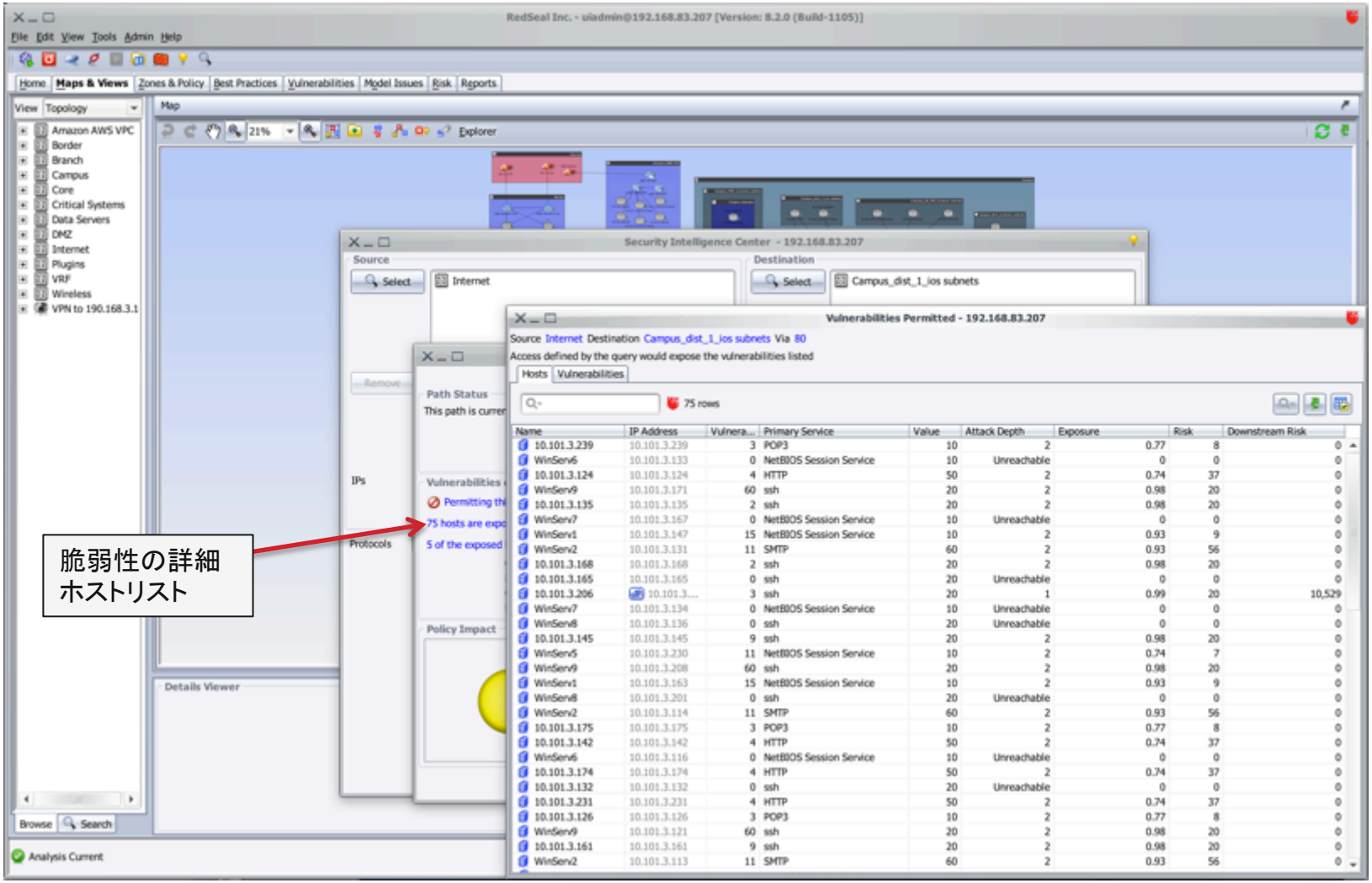
Security Intelligence Center – Security Impact Query



Security Intelligence Center – Security Impact Query



Security Intelligence Center – Security Impact Query



Security Intelligence Center – Security Impact Query