

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

デバイスの接続情報、又は  
CMDBやファイルサーバーの  
接続情報を定義する

収集方法を  
指定する

The screenshot shows the 'Data Import - 192.168.83.207' application window. The 'File Import' tab is active. Below it, the 'Data Collection Task' dialog is open. The 'Data type' section has 'L2 & L3 Devices' selected. A list of device types is shown, with 'Cisco IOS (8.2.0)' selected. The 'Communication Method' dropdown is set to 'SSH'. The 'Details for Selected Plug-In Pair' section shows 'Data Plug-in: Cisco IOS' and 'Communication Plug-in: SSH'. The 'Hostname' field contains '172.16.10.1' and the 'Port' field contains '22'. The 'Schedule' tab is selected in the 'Details' section.

# 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

The screenshot shows the RedSeal Best Practices interface. At the top, there are tabs for 'Checks' and 'Suppressions'. Below this, a search bar and a 'Show All Checks' checkbox are visible. The main table lists various checks with columns for Check ID, Title, Severity, Passed Devices, Failed Devices, Violation Instances, and Platforms. A red arrow points to the 'Show All Checks' checkbox, another to the 'Severity' column header, and a third to the 'Platforms' column header. Below the main table, there is a section for 'No Enable Secret' with a 'View by Violation' button and a search bar. This section displays a detailed table with columns for Status, Name, Device Type, Operating System, and Modified. A red arrow points to the 'Operating System' column in this detailed view. At the bottom right, there is a status bar showing 'Client 244 M of 982 M' and 'Server 2,692 M of 3,944 M'.

| Check ID     | Title  | Severity | Passed Devices | Failed Devices | Violation Insta... | Platforms              |
|--------------|--|----------|----------------|----------------|--------------------|------------------------|
| RS-36        | IP Source Routing Enabled                                | HIGH     | 12             | 39             | 39                 | Juniper JunOS          |
| RS-37        | No Enable Secret   | HIGH     | 2              | 31             | 31                 | Cisco IOS              |
| RS-16        | Unencrypted Passwords                                    | HIGH     | 35             | 3              | 3                  | Cisco IOS              |
| RS-55        | No Password on Console                                   | HIGH     | 30             | 3              | 3                  | Cisco IOS              |
| RS-32        | Weak Community String                                    | HIGH     | 47             | 2              | 2                  | Cisco PIX - ASA - FWSM |
| NET0600      | Passwords are viewable when displaying the config.       | HIGH     | 0              | 2              | 2                  | Cisco IOS              |
| NET0927      | RFC 1918 addresses are not blocked                       | HIGH     | 0              | 2              | 2                  | Cisco IOS              |
| NET0230      | Network element is not password protected.               | HIGH     | 0              | 2              | 2                  | Cisco IOS              |
| NET0230      | Network element is not password protected                | HIGH     | 0              | 2              | 2                  | Cisco PIX - ASA - FWSM |
| NET0950      | uRPF strict mode or ACL not enabled on egress interface. | HIGH     | 0              | 2              | 2                  | Cisco IOS              |
| NET1636      | Management connections must require passwords.           | HIGH     | 0              | 2              | 2                  | Cisco PIX - ASA - FWSM |
| NET-NAC-009  | NET-NAC-009  | HIGH     | 0              | 2              | 2                  | Cisco IOS              |
| NET1660      | An insecure version of SNMP is being used.               | HIGH     | 0              | 2              | 2                  | Cisco IOS              |
| NET0923      | IPv4 Loopback address is not blocked                     | HIGH     | 0              | 2              | 2                  | Cisco IOS              |
| NET-TUNL-020 | Teredo is not blocked by filtering UDP port 3544         | HIGH     | 0              | 2              | 2                  | Cisco IOS              |
| NET1623      | Authentication required for console access.              | HIGH     | 0              | 2              | 2                  | Cisco PIX - ASA - FWSM |
| NET1636      | Management connections must require passwords.           | HIGH     | 0              | 2              | 2                  | Cisco IOS              |

| Status | Name                  | Device Type | Operating System | Modified                 |
|--------|-----------------------|-------------|------------------|--------------------------|
| Failed | Branch-Corp-Texas-ios | Router      | IOS 12.1         | Jan 28, 2016 12:10:33 PM |
| Failed | Data-2-ios            | Router      | IOS 12.1         | Oct 16, 2012 3:09:33 PM  |
| Failed | Campus-Dev-ios        | Router      | IOS 12.1         | Oct 16, 2012 3:09:38 PM  |
| Failed | Plugins-ios           | Router      | IOS 12.1         | Oct 16, 2012 3:09:22 PM  |
| Failed | test                  | Router      | IOS 12.1         | Oct 16, 2012 3:09:45 PM  |
| Failed | product               | Router      | IOS 12.1         | Oct 16, 2012 3:09:45 PM  |
| Failed | ios-wf-ios            | Router      | IOS 12.1         | Oct 16, 2012 3:09:25 PM  |
| Failed | Branch-dist-ios       | Router      | IOS 12.1         | Oct 16, 2012 3:09:42 PM  |
| Failed | ios-wf-rd-ios         | Router      | IOS 12.1         | Oct 16, 2012 3:09:16 PM  |
| Failed | Data-1-ios            | Router      | IOS 12.1         | Oct 16, 2012 3:09:35 PM  |
| Failed | DMZ-srv-3-ios         | Router      | IOS 12.1         | Oct 16, 2012 3:09:30 PM  |

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

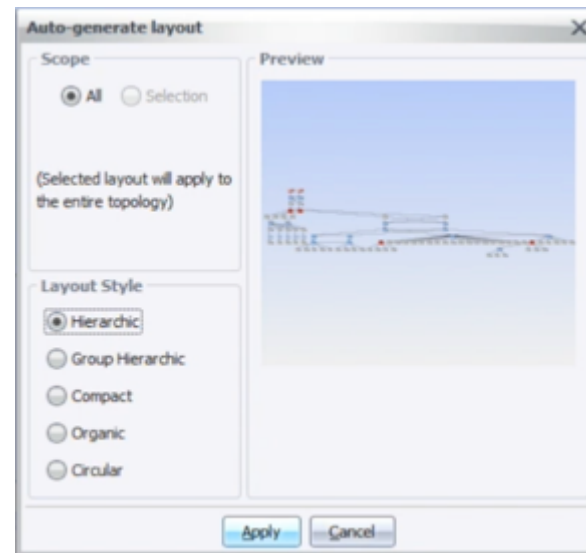
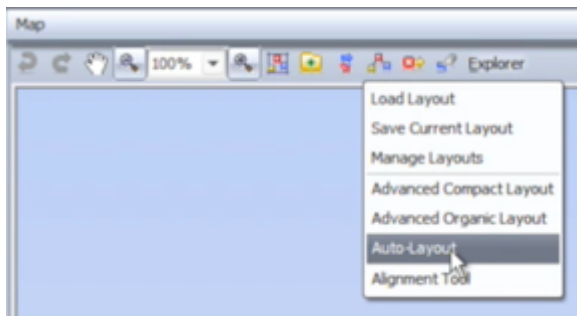
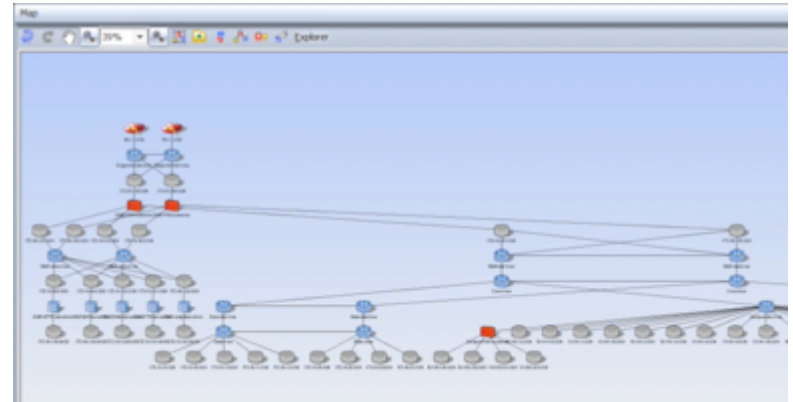
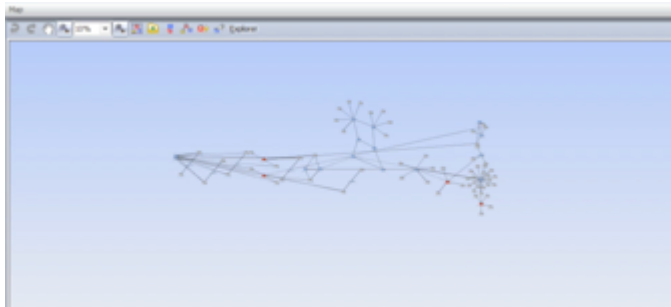
(行数が表示されていると) 右クリック | Show in Config Fileでコンフィグ内で確認

# 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

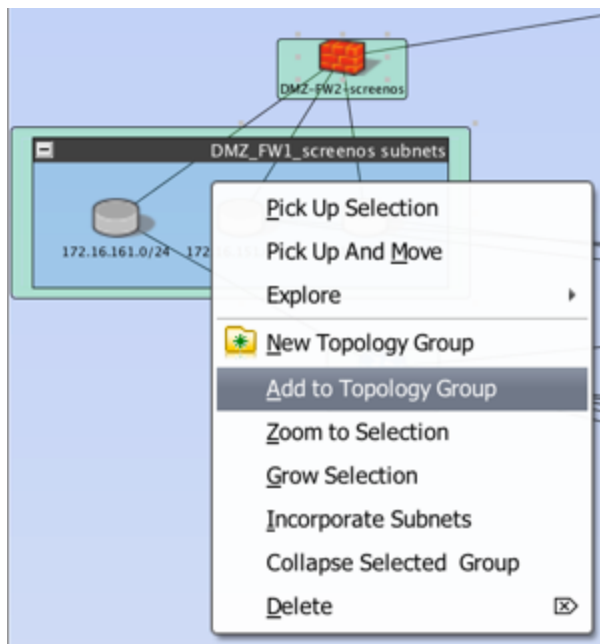
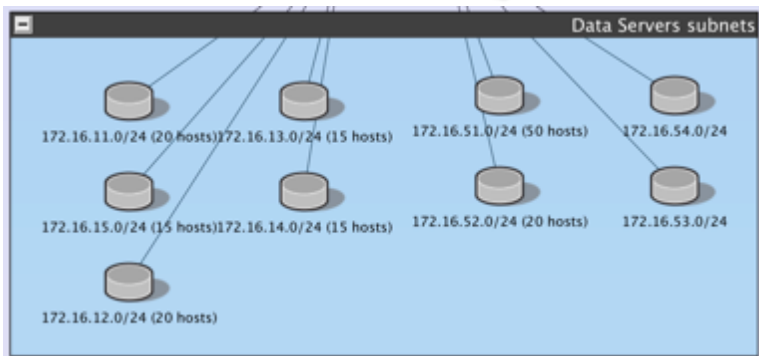
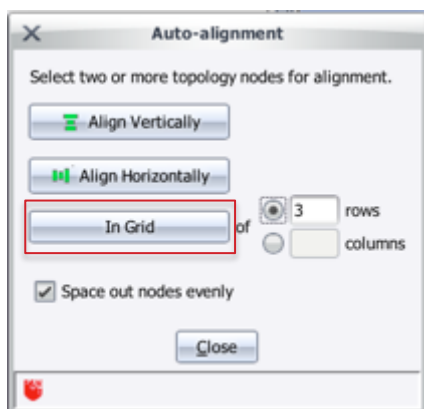
- Auto-Layout ツールを使い、グループの作成作業を開始する





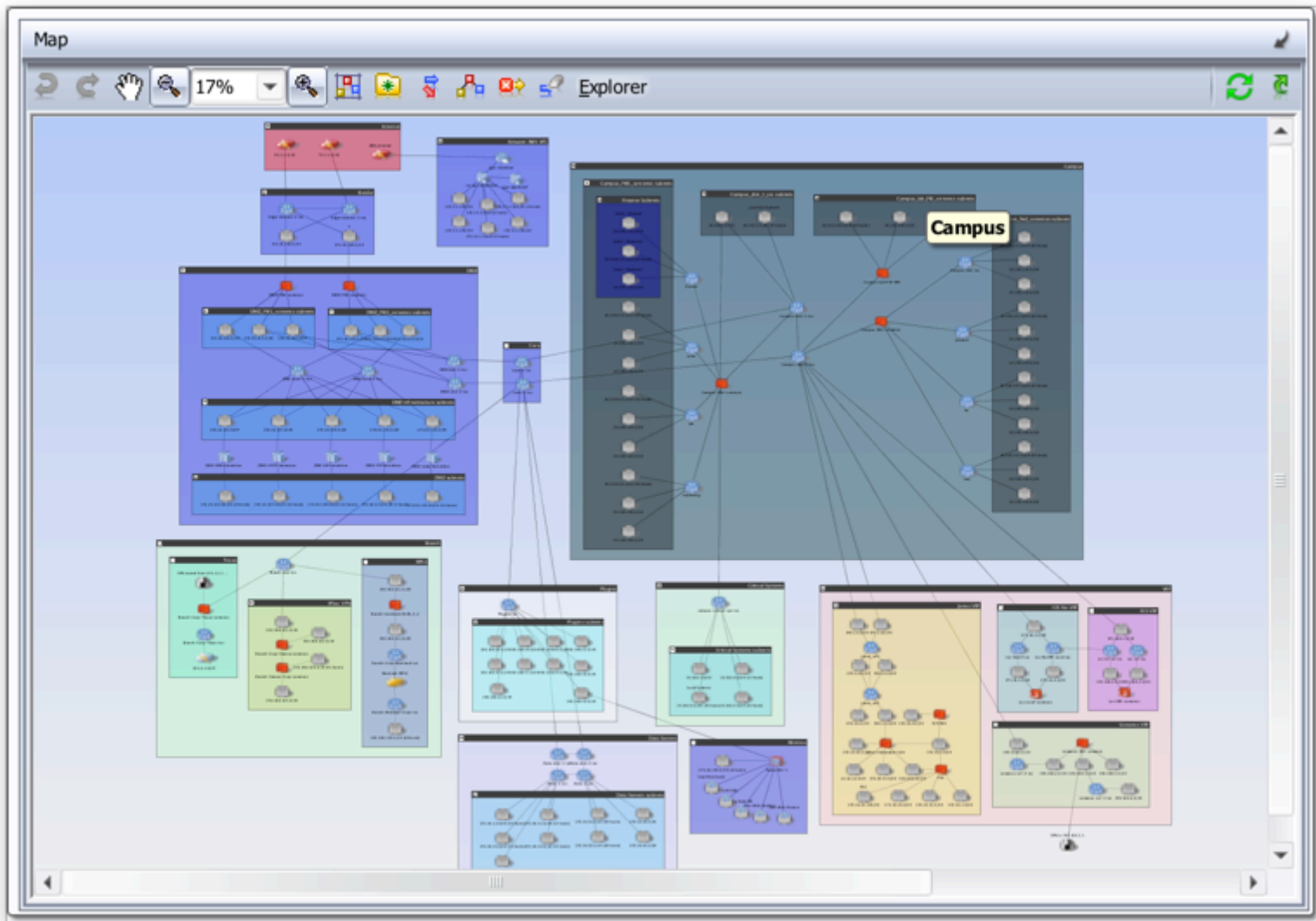
# Topology Layout

- 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

The screenshot shows the RedSeal Model Issues interface. At the top, there's a menu bar with 'File', 'Edit', 'View', 'Tools', 'Admin', and 'Help'. Below it are tabs for 'Home', 'Maps & Views', 'Zones & Policy', 'Best Practices', 'Vulnerabilities', 'Model Issues', 'Risk', and 'Reports'. The 'Model Issues' tab is active, showing a 'Checks' section with a search bar and '19 rows'. A table lists various checks with columns for 'Check ID', 'Title', 'Severity', and 'Violation Instances'. The first two rows are MI-1 (Overlapping Subnets, HIGH, 2) and MI-2 (Duplicate VLAN Number, MEDIUM, 2). A red arrow points to these two rows with the text '最低限この二つのMIを解決する'. Below the table, the 'Overlapping Subnets' section is expanded, showing an 'Explanation' and 'Remediation' section. A red bracket groups this section with the text 'Model Issueの詳細と解決案'. Below that, a table shows details for two overlapping subnets, with a red bracket pointing to it and the text 'Model Issueの詳細: ここからEdit Subnet'. The bottom of the interface shows 'Analysis Current' and client/server statistics.

| Check ID | Title                          | Severity | Violation Instances |
|----------|--------------------------------|----------|---------------------|
| MI-1     | Overlapping Subnets            | HIGH     | 2                   |
| MI-2     | Duplicate VLAN Number          | MEDIUM   | 2                   |
| MI-3     | Colliding IP Addresses         | HIGH     | 1                   |
| MI-4     | Unmapped Hosts                 | HIGH     | 20                  |
| MI-5     | Dangling Links                 | HIGH     | 2                   |
| MI-6     | Unnumbered Unlinked Interfaces | HIGH     | 15                  |
| MI-7     | Unscanned Host-Subnets         | HIGH     | 80                  |
| MI-8     | Stale Devices                  | HIGH     | 50                  |
| MI-9     | Stale Hosts                    | HIGH     | 1,256               |
| MI-10    | Unplaced Transparent Firewalls | HIGH     | 2                   |

**Overlapping Subnets**

**Explanation**

**Description:** Overlapping subnets have been detected. This can indicate a serious network misconfiguration, causing hosts in either subnet to be unreachable from some parts of the network. If intentional (two isolated parts of the network legitimately using similar address space), you should limit the configurations loaded into RedSeal to a subset of the network that excludes overlaps in internal addressing.

**Remediation:** Do one of the following:

- Move devices or hosts from one subnet to another (right click on a subnet in the table, select Edit Subnet | Split Subnet)
- Delete offending computer systems which are no longer part of your network (expand the table row to show devices, right click, select Delete Computer Systems)

| Summary  | First Noticed           |                 |
|--|-------------------------|-----------------|
| Subnet "172.16.32.0/24" (defined on interface fe-0/0/2.0 of device junos-redundant-rule) overlaps a... | Sep 28, 2015 3:59:35 AM |                 |
| Subnet   | Type                    | Number of hosts |
| + 172.16.32.128/26 PA1   | Trusted                 | 0               |
| + 172.16.32.0/24   | Trusted                 | 0               |
| Subnet "172.16.2.0/24 (external)" (defined on interface eth0 of device R71FW3) overlaps address sp...  | Jul 10, 2015 4:15:21 AM |                 |
| Subnet   | Type                    | Number of hosts |
| + 172.16.2.0/24 (external)   | Trusted                 | 0               |
| + 172.16.2.0/30 (connected to Data-2-ios)  | Trusted                 | 0               |

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

Likely Threat Sources - 192.168.83.207

This table contains all subnets the RedSeal server considers likely to be untrusted regardless of their current trust level, including any subnets you have already designated as untrusted.

Show All Subnets

Select one or more subnets in the table and use the right-click menu to set the desired trust level.

⚠ = unsaved

Q- 🔴 26 rows

| Trust L... | Name                                   | Likely Reason               | Description            | Devices                 | Hosts |
|------------|--|-----------------------------|------------------------|-------------------------|-------|
| Trusted    | User Role HR                           | One ended unnumbered subnet | User Role HR           | Aruba-WC-1              | 0     |
| Trusted    | VPN tunnel from 101.1.1.1 to 102.1.... | One ended unnumbered subnet | Untrust                | Branch-Corp-Texas-sc... | 0     |
| Trusted    | User Role Sales                        | One ended unnumbered subnet | User Role Sales        | Aruba-WC-1              | 0     |
| Internet   | 80.1.1.0/24 (connected to internet2)   | Set as Untrusted            | connected to internet2 | Edge-Internet-2-los     | 0     |
| Trusted    | User Role Auditors                     | One ended unnumbered subnet | User Role Auditors     | Aruba-WC-1              | 0     |
| Trusted    | User Role Guest                        | One ended unnumbered subnet | User Role Guest        | Aruba-WC-1              | 0     |
| Trusted    | 192.168.122.0/24 (Untrust)             | Defined as outside          | Untrust                | Branch-Corp-Vienna-s... | 0     |
| Extranet   | 101.2.1.0/24 (connected to extranet)   | Set as Untrusted            | connected to extranet  | Branch-Corp-Texas-los   | 0     |

Save Cancel Help

Analysis Current

Client 181 M of 993 M  
Server 3,164 M of 3,944 M



# 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なる
  - ファイアウォールルール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

The screenshot shows the RedSeal Inc. web interface with the following components:

- Navigation:** Home, Maps & Views, Zones & Policy, Best Practices, Vulnerabilities, Model Issues, Risk, Reports.
- RedSeal Model Status:** Last Inventory Update Mar 16, 2016 5:52:20 PM. Includes counts for Network Devices (68), Hosts (1,264, 1,256 stale), Threat Sources (4), and Model Issues (1,461 +0).
- Best Practices Analysis:** Total Check Violations: 697. Bar chart showing counts for HIGH, MEDIUM, and LOW severity levels. Changes since 1 Week ago: 317 new (red up arrow), 8 resolved (green down arrow).
- Network Policy Compliance:** Details... button and six pie charts for PCI Audit, External-Internal, Finance, Montreal to Campus F..., NERC-CIP Policy, and NERC Example Policy.
- Risk Analysis:** Details... button and a flow diagram showing Untrusted (red sphere) leading to Direct Attacks (197 hosts) and Indirect Attacks (423 hosts), which then lead to Protected (624 hosts).
- Overall Health:** Alerts All. Latest scheduled data collection failed.
- Footer:** Analysis Outdated. Operation complete, 1 Succeeded. Client 225 M of 972 M, Server 1,700 M of 3,944 M.

# 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

The screenshot displays the RedSeal network management interface. On the left, a tree view shows various network components like Amazon AWS VPC, Border, Branch, Campus, Core, Critical Systems, Data Servers, DMZ, Internet, Plugins, VRF, Wireless, and VPN to 190.168.3.1. The main area shows a complex network topology map with nodes and connections. A context menu is open over a node, listing options such as Explore, Edit, Show Layer 2 Map, New Topology Group, Add to Topology Group, Zoom to Selection, Grow Selection, Incorporate Subnets, Add Notation, and Show Layer 2 Web Map. A sub-menu is also visible, containing 'Access From', 'Access To', 'Threats From', 'Threats To', 'Set as destination', and 'Set as source'. A red arrow points from a callout box to the 'Access From' option. The callout box contains the text: 'Explore機能を使った簡易的なアクセスクエリー'. At the bottom, there is a status bar with 'Analysis Current', 'Operation complete, 1 Succeeded. Click here for details.', and resource usage information: 'Client 209 M of 977 M' and 'Server 2,360 M of 3,944 M'.

# Access Queries – 検証や調査等の場合

Toolsメニューから  
Security Intelligence  
Centerを選択

The screenshot shows the RedSeal Security Intelligence Center interface. The main window is titled "Security Intelligence Center - 192.168.83.207". It features a "Source" field with a "Select" button and "Internet" as the selected value. The "Destination" field also has a "Select" button and "Campus\_dist\_1\_ios subnets" as the selected value. Below these fields are "IPs" and "Protocols" sections, both with "Optional" dropdowns and "All IPs" selected. There are "Remove" buttons for both source and destination. At the bottom, there is an "Analyze Query" section with buttons for "Access", "Threats", "Policy Status", "Security Impact", and "Detailed Path". A red arrow points from the "Tools" menu in the top-left corner to the "Security Intelligence Center" option. Another red arrow points from the "Select" button in the Source field to the text "アクセスの照会条件を特定する". A third red arrow points from the "Analyze Query" button to the text "アクセスクエリーを実行する". The interface also shows a "Map" view on the right and a status bar at the bottom indicating "Analysis Current Operation complete, 1 Succeeded. Click here for details."

アクセスの照会条件を特定する

アクセスクエリーを実行する

# Access Queries – レポート出力の為のクエリー構築

The screenshot shows the Security Query Manager interface. The top menu bar includes File, Edit, View, Tools, and Add. The left sidebar shows a tree view of network components like Amazon AWS VPC, Border, Branch, Campus, Core, Critical Systems, Data Servers, DMZ, Internet, Routers, VRF, Wireless, and VPN to 190.168.1.1. The main window displays a table of saved queries with columns for Name, Type, Tracking, and Used by Reports. The 'Known Attack Surface Access' query is selected. Below the table, the configuration panel for this query is shown, including Source (All Untrusted Subnets), Destination (All Trusted Subnets), and various options like Track, Protocols, and Ports. The 'Track' checkbox is checked.

| Name                               | Type            | Tracking | Used by Reports |
|------------------------------------|-----------------|----------|-----------------|
| 10.101.3.206 to 10.100.113.114     | Access          | false    |                 |
| Known Attack Surface Access        | Access          | true     |                 |
| Known Attack Surface Access (copy) | Access          | true     |                 |
| Known Critical Assets Access       | Access          | true     |                 |
| Known DMZ Bypass Access            | Access          | true     |                 |
| Known DMZ Outlets Access           | Access          | true     |                 |
| Potential Attack Surface Access    | Access          | true     |                 |
| Potential Critical Assets Access   | Access          | true     |                 |
| Potential DMZ Bypass Access        | Access          | true     |                 |
| Potential DMZ Outlets Access       | Access          | true     |                 |
| securityimpact1017014440           | Security Impact | false    |                 |
| securityimpact188881418            | Security Impact | false    |                 |
| securityimpact204906391            | Security Impact | false    |                 |
| securityimpact216309860            | Security Impact | false    |                 |
| securityimpact421406334            | Security Impact | false    |                 |
| securityimpact462154354            | Security Impact | false    |                 |

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

Trackが選択されると履歴が記録される

# 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)

The screenshot displays the RedSeal PCI Audit software interface. The main window shows a network diagram with several zones: Untrusted, General, DMZ, Wireless, Cardholder, and Out of Scope. The diagram uses colored arrows to represent traffic flow: green for 'Pass No Flow', yellow for 'Pass', red for 'Fail', and dashed red for 'Zone Overlap'. The 'Untrusted' zone is at the top, connected to 'General' and 'DMZ'. 'General' and 'DMZ' are connected to each other and to 'Wireless' and 'Cardholder'. 'Wireless' and 'Cardholder' are connected to each other. 'Out of Scope' is a separate zone. The interface includes a menu bar, a toolbar, and a sidebar with a 'Policy' dropdown menu. The status bar at the bottom indicates 'Analysis Current: Operation complete, 1 Succeeded. Click here for details.' and shows client/server memory usage.

ドリップダウンからポリシーを選択

PCI-DSS ポリシーはデフォルトで搭載済み

新しいポリシーを構築する

Table Export

Manage Policy Sets

Deactivate Policy

Show

Rules

Compliance

Reports

Rules

PCI Compliance

PCI Audit Compliance

Pass No Flow

Pass

Warning

Fail

Zone Overlap

View

Name: PCI Audit

Policy Active: true

Policy Editable: false

User Editable: false

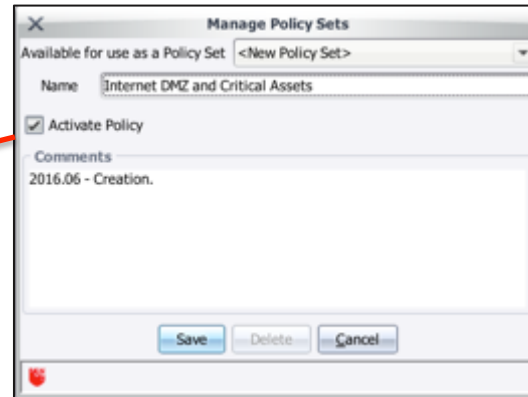
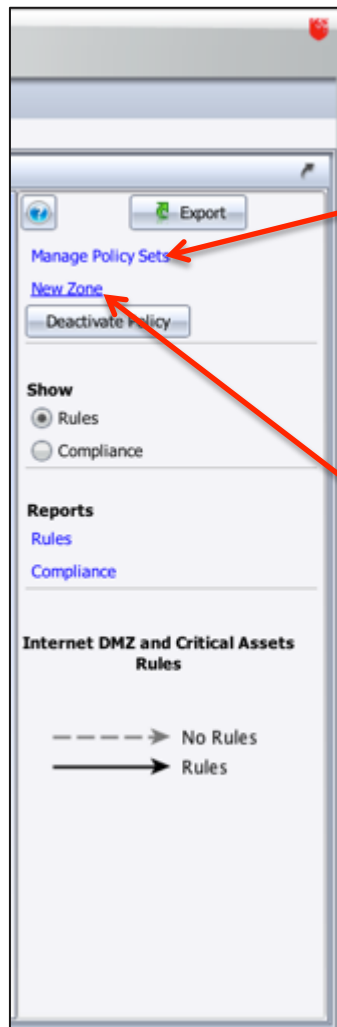
Analysis Current: Operation complete, 1 Succeeded. Click here for details.

Client 107 M of 979 M

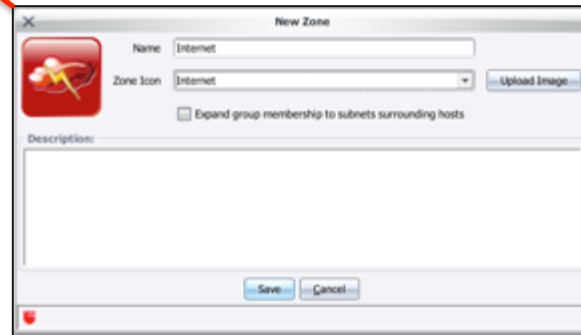
Server 2,013 M of 3,944 M



# Security Segmentation (Zones & Policy)

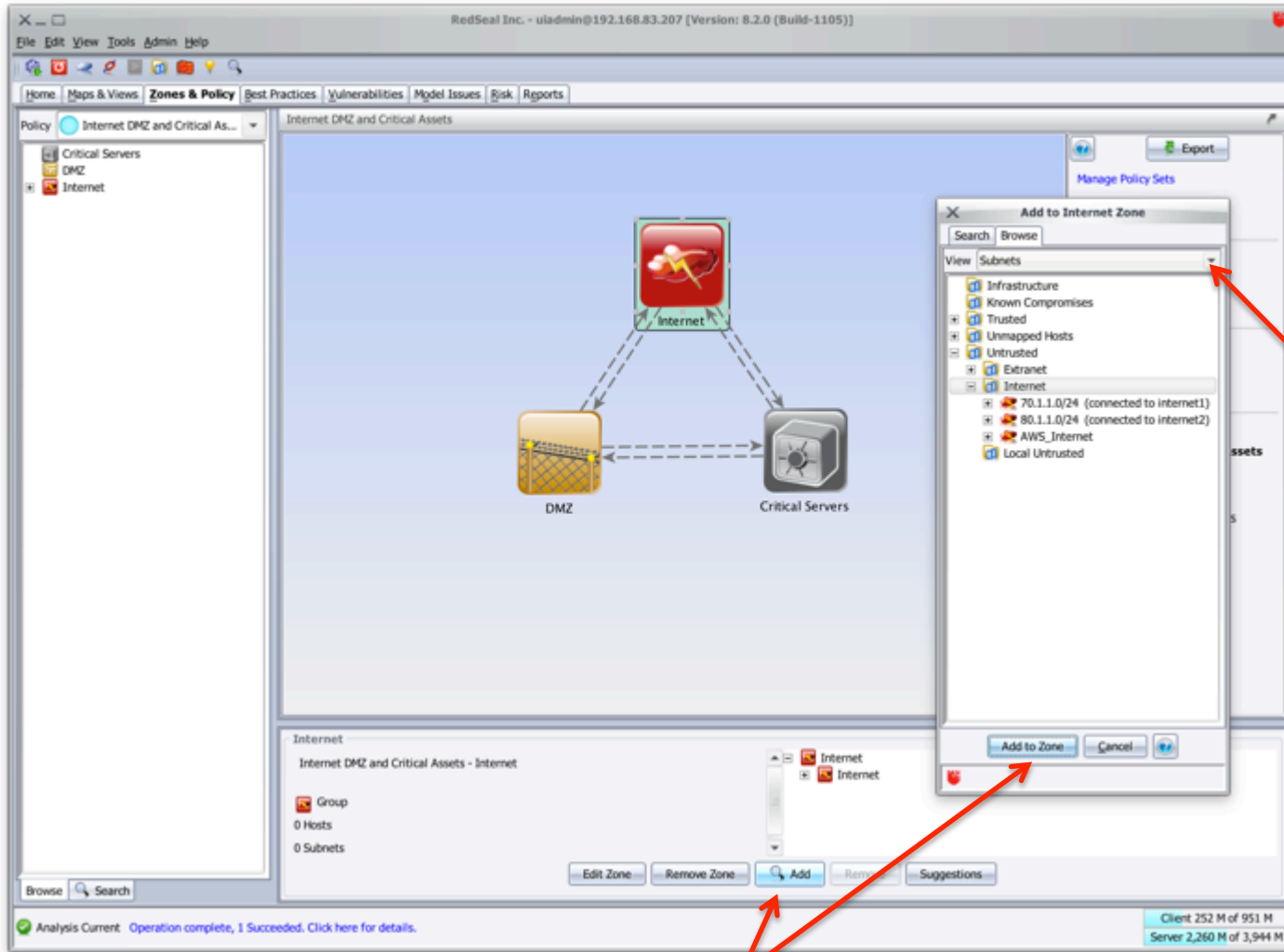


Manage Policy Setsから  
新規ポリシーを構築



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)

The screenshot displays the RedSeal Security Segmentation interface. The main window shows a network diagram with three zones: Internet (red lightning bolt icon), DMZ (yellow fence icon), and Critical Servers (grey server icon). Dashed arrows indicate connections between Internet and DMZ, Internet and Critical Servers, and DMZ and Critical Servers. A yellow arrow points from the Internet zone to the Critical Servers zone, with a red arrow pointing to it from the text 'Zone間の矢印を選択し、Edit Rulesをクリックしてアクセスルールを定義'. Below the diagram is a dialog box titled 'Edit Rules for Internet DMZ and Critical Assets'. The dialog has 'Source Zone' set to 'Internet' and 'Destination Zone' set to 'Critical Servers'. Under 'Rules from Internet to Critical Servers', the 'Access rule' section has 'Enable access rule' checked, and 'All access forbidden' selected. The 'Firewall rule' section has 'Firewalls required' checked. A red arrow points from the text 'Only test zone overlap:' to the 'Only test zone overlap' radio button. Another red arrow points from the text 'Approvals required:' to the 'Approvals required' radio button. A third red arrow points from the text 'All Access Forbidden:' to the 'All access forbidden' radio button. The dialog has 'Save' and 'Cancel' buttons. On the right side of the main window, there are buttons for 'Export', 'Manage Policy Sets', 'New Zone', and 'Deactivate Policy'. Below these are sections for 'Show' (Rules, Compliance), 'Reports' (Rules, Compliance), and 'Internet DMZ and Critical Assets Rules'. A legend shows a dashed arrow for 'No Rules' and a solid arrow for 'Rules'. At the bottom right, there is a status bar showing 'Client 162 M of 955 M' and 'Server 2,380 M of 3,944 M'.

Zone間の矢印を選択し、  
Edit Rulesをクリックして  
アクセスルールを定義

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

Rules  
Source Zone: Internet  
Destination Zone: Critical Servers  
Status: No Rules

Edit Rules

Client 162 M of 955 M  
Server 2,380 M of 3,944 M

# Security Segmentation (Zones & Policy)

RedSeal Inc. - uladmin@192.168.83.207 [Version: 8.2.0 (Build-1105)]

File Edit View Tools Admin Help

Home Maps & Views **Zones & Policy** Best Practices Vulnerabilities Model Issues Risk Reports

Policy Internet DMZ and Critical As...

Critical Servers  
DMZ  
Internet

Internet DMZ and Critical Assets

Internet  
DMZ  
Critical Servers

Export

Manage Policy Sets  
New Zone  
Deactivate Policy...

Show  
 Rules  
 Compliance  
**Update Compliance**

Reports  
Rules  
Compliance

Internet DMZ and Critical Assets Rules

---> No Rules  
-> Rules

View  
Name: Internet DMZ and Critical Assets  
Policy Active: true  
Policy Editable: true  
User Editable: true

Browse Search

Analysis Current Operation complete, 1 Succeeded. Click here for details.

Client 235 M of 958 M  
Server 1,848 M of 3,944 M

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)

The screenshot displays the RedSeal Security Segmentation interface. The top part shows a network diagram with three zones: Internet (red), DMZ (yellow), and Critical Servers (grey). Arrows indicate traffic flow: a green arrow from Internet to DMZ, a green arrow from Internet to Critical Servers, a yellow arrow from DMZ to Critical Servers, and a red arrow from Critical Servers to DMZ. A red arrow points to the red arrow in the diagram with the text "矢印を選択し、画面下で詳細を確認する".

The bottom part shows a table titled "Internet DMZ and Critical Assets Firewall Status from From Critical Servers to DMZ". The table has 8 columns: Source Zone, Destination Zone, Source Subnet, Firewall, Spoof Filter, Best Practices, Destination, Policy Status, and Ticket. The Policy Status column shows "No Firewall" for all four rows, with a red 'X' icon next to each entry. A red arrow points to the "No Firewall" entries with the text "ここからDetailed Pathのクエリーを実施して確認作業が行える".

On the right side, there is a legend for the compliance results:

- Pass No Flow (green dashed arrow)
- Pass (green solid arrow)
- Warning (yellow solid arrow)
- Fail (red solid arrow)
- Zone Overlap (red dashed line)

Text on the right side of the image says "セグメンテーション確認の結果が色別で表示される" with a red arrow pointing to the legend.

At the bottom of the interface, there is a status bar: "Analysis Current Operation complete, 1 Succeeded. Click here for details." and a memory usage indicator: "Client 121 M of 959 M Server 2,264 M of 3,944 M".

セグメンテーション確認の結果が色別で表示される

矢印を選択し、画面下で詳細を確認する

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するの詳細は  
*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

The screenshot displays the RedSeal Security Intelligence Center interface. The main window is titled "RedSeal Inc. - vladim@192.168.83.207 (Version: 8.2.0 (Build-1189))". The interface is divided into several sections:

- Top Panel:** Contains navigation tabs for "Home", "Maps & Views", "Zones & Policy", "Test Practices", "Vulnerabilities", "Hybrid Issues", "Risk", and "Reports".
- Left Panel:** Includes "Information" (explaining Down Stream Risk [DSR]), "Risk Map Controls", and "Analysis Current" status.
- Center Panel:** Displays a "RedSeal Risk Map" with a grid of colored boxes representing hosts. A "Details Viewer" is located below the map.
- Right Panel:** Shows a list of "High Risk Vulnerabilities" with columns for CVE ID, Description, Host c., Total Vuln., Severity, and Ticket.
- Bottom Panel:** Contains a table of host details with columns for Host Name, IP, Application, Protocols, Ports, Scan Date, Risk, and Downstream.

A "Threats From/To" popup is overlaid on the interface, showing a network diagram and a summary of vulnerabilities:

- Explore**
- Edit**
- Show Layer 2 Map**
- New Topology Group**
- Access From**
- Access To**
- Threats From**
- Threats To**

**Vulnerabilities on the Destination**

- Permitting this access exposes 795 vulnerabilities.
- 75 hosts are exposed in the destination.
- 50 of the exposed hosts have leapfrog vulnerabilities.
- Oldest scan date: Jul 27, 2004
- Number of unique vulnerabilities: 81
- Collective impact: ACIS
- Max CVSS base score: 10.0

# Vulnerability Management

The screenshot shows the RedSeal interface with a network topology map at the top and a detailed host vulnerability table below. The table lists various hosts with their IP addresses, primary services, and associated risk metrics.

| Name         | IP Address   | Vulnerabil... | 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               |
| WinServ4     | 10.101.3.163 | 15            | NetBIOS Session Service | 10    | 2            | 0.93     | 9    | 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               |
| WinServ4     | 10.101.3.162 | 15             | NetBIOS Session Service | 10    | 2            | 0.93     | 9    | 0               |

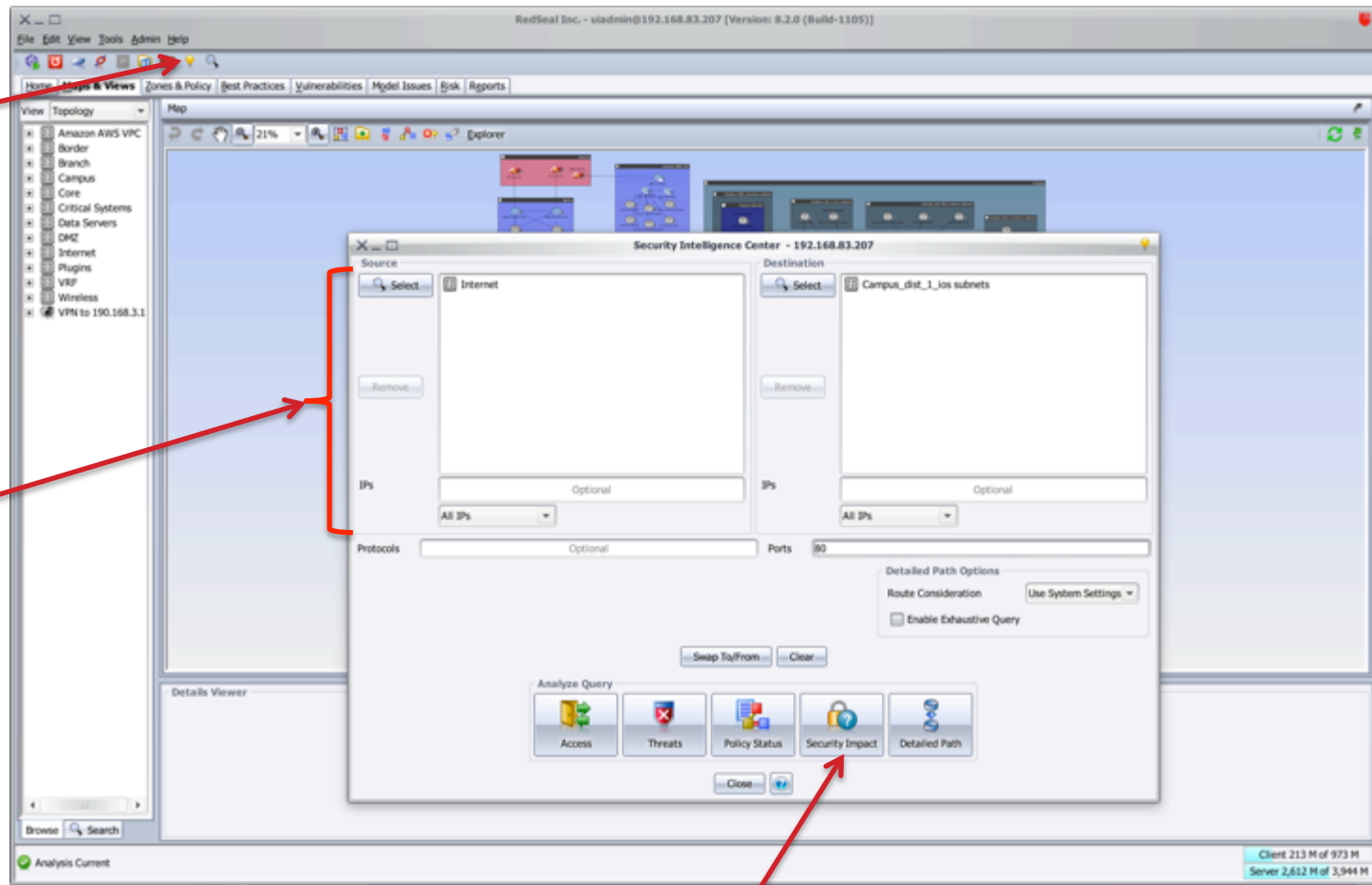
# Security Intelligence Center – Security Impact Query

- 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立つ機能
  - 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

検証されたパスがOPENかBLOCKEDか？  
Detailed Pathでパスを確認(例: 何処でBlockされているか、等)

パスがOPENの場合に露出される脅威

検証されたパスがどのポリシーに影響を及ぼすのか？  
黄色: アクセス認証要  
赤: ポリシー違反

Source: Internet  
Destination: Campus\_dist\_1\_ios subnets  
Via: 80

Path Status: This path is currently **BLOCKED**

Exposure:  
Source: Untrusted  
Destination: Indirectly Attackable

Vulnerabilities on the Destination:  
Permitting this access exposes **55 vulnerabilities**.  
75 hosts are exposed in the destination.  
5 of the exposed hosts have leapfrog vulnerabilities.

Downstream Impact:  
Source: 10.101.3.124, 10.101.3.142, 10... Destination: All Trusted Subnets  
761 hosts would be reachable via leapfrog vulnerabilities.

Policy Impact:  
External-Internal: Details New Decision  
NERC-CIP Policy: Details New Decision  
PCI AudR: Details New Decision

# Security Intelligence Center – Security Impact Query

The screenshot displays the RedSeal Security Intelligence Center (SIC) interface. The main window shows a network topology map with various nodes and connections. Overlaid on this is a 'Security Intelligence Center - 192.168.83.207' window. This window has a 'Source' field set to 'Internet' and a 'Destination' field set to 'Campus\_dist\_1\_ios subnets'. Below this, a 'Vulnerabilities Permitted - 192.168.83.207' window is open, showing a table of vulnerabilities. The table has columns for Vulnerability, Host Name, IP, Application, Ports, Risk, Downst..., Atta..., Type, Exposed, Leapfrog, CV..., and Tic... The table lists 55 rows of vulnerability data. A red arrow points from a text box to the 'Vulnerabilities' tab in the SIC window.

脆弱性の詳細  
CVE-IDリスト

| Vulnerability | Host Name    | IP           | Application                    | Ports | Risk | Downst... | Atta... | Type      | Exposed   | Leapfrog | CV... | Tic... |
|---------------|--------------|--------------|--------------------------------|-------|------|-----------|---------|-----------|-----------|----------|-------|--------|
| CVE-2003-0226 | ManServ2     | 10.101.3.160 | Microsoft IIS HTTP 5.1 Fron... | 80    | 30   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-2003-0020 | 10.101.3.142 | 10.101.3.142 | Apache 1.3.x HTTP              | 80    | 37   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-2001-0151 | ManServ2     | 10.101.3.246 | Microsoft IIS HTTP 5.1 Fron... | 80    | 30   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-2002-0419 | ManServ2     | 10.101.3.160 | Microsoft IIS HTTP 5.1 Fron... | 80    | 30   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-2002-0419 | WirServ2     | 10.101.3.114 | Microsoft IIS HTTP 6.0 Fron... | 80    | 56   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-2002-0419 | WirServ2     | 10.101.3.164 | Microsoft IIS HTTP 6.0 Fron... | 80    | 56   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-2002-0419 | WirServ2     | 10.101.3.113 | Microsoft IIS HTTP 6.0 Fron... | 80    | 56   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-2001-0151 | ManServ2     | 10.101.3.127 | Microsoft IIS HTTP 5.1 Fron... | 80    | 30   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-2001-1013 | 10.101.3.174 | 10.101.3.174 | Apache HTTP                    | 80    | 37   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-2002-0392 | 10.101.3.158 | 10.101.3.158 | Apache HTTP                    | 80    | 37   | 0         | 2       | CONFIR... | Subnet... | Yes      | 7.5   |        |
| CVE-2002-0419 | ManServ2     | 10.101.3.144 | Microsoft IIS HTTP 5.1 Fron... | 80    | 30   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-2001-0151 | ManServ2     | 10.101.3.176 | Microsoft IIS HTTP 5.1 Fron... | 80    | 30   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-2003-0460 | 10.101.3.174 | 10.101.3.174 | Apache 1.3.x HTTP              | 80    | 37   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-2003-0020 | 10.101.3.174 | 10.101.3.174 | Apache 1.3.x HTTP              | 80    | 37   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-2002-1182 | ManServ2     | 10.101.3.160 | Microsoft IIS HTTP 5.1 Fron... | 80    | 30   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-1999-0386 | WirServ2     | 10.101.3.114 | Microsoft IIS HTTP 6.0 Fron... | 80    | 56   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-1999-0386 | ManServ2     | 10.101.3.246 | Microsoft IIS HTTP 5.1 Fron... | 80    | 30   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-1999-0386 | WirServ2     | 10.101.3.148 | Microsoft IIS HTTP 6.0 Fron... | 80    | 56   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-1999-0386 | ManServ2     | 10.101.3.127 | Microsoft IIS HTTP 5.1 Fron... | 80    | 30   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-1999-0386 | ManServ2     | 10.101.3.144 | Microsoft IIS HTTP 5.1 Fron... | 80    | 30   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-2002-0392 | 10.101.3.124 | 10.101.3.124 | Apache HTTP                    | 80    | 37   | 0         | 2       | CONFIR... | Subnet... | Yes      | 7.5   |        |
| CVE-2001-1013 | 10.101.3.142 | 10.101.3.142 | Apache HTTP                    | 80    | 37   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-2001-1013 | 10.101.3.231 | 10.101.3.231 | Apache HTTP                    | 80    | 37   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-2002-0419 | ManServ2     | 10.101.3.176 | Microsoft IIS HTTP 5.1 Fron... | 80    | 30   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-1999-0386 | WirServ2     | 10.101.3.131 | Microsoft IIS HTTP 6.0 Fron... | 80    | 56   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-2002-0419 | ManServ2     | 10.101.3.127 | Microsoft IIS HTTP 5.1 Fron... | 80    | 30   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-2002-0419 | ManServ2     | 10.101.3.246 | Microsoft IIS HTTP 5.1 Fron... | 80    | 30   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |
| CVE-2002-0392 | 10.101.3.174 | 10.101.3.174 | Apache HTTP                    | 80    | 37   | 0         | 2       | CONFIR... | Subnet... | Yes      | 7.5   |        |
| CVE-2003-0460 | 10.101.3.124 | 10.101.3.124 | Apache 1.3.x HTTP              | 80    | 37   | 0         | 2       | CONFIR... | Subnet    | No       | 5     |        |

# Security Intelligence Center – Security Impact Query

脆弱性の詳細  
ホストリスト

| Name         | IP Address   | Vulnera... | 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               |
| WinServ1     | 10.101.3.163 | 15         | NetBIOS Session Service | 10    | 2            | 0.93     | 9    | 0               |
| WinServ8     | 10.101.3.201 | 0          | ssh                     | 20    | Unreachable  | 0        | 0    | 0               |
| WinServ2     | 10.101.3.114 | 11         | SMTP                    | 60    | 2            | 0.93     | 56   | 0               |
| 10.101.3.175 | 10.101.3.175 | 3          | POP3                    | 10    | 2            | 0.77     | 8    | 0               |
| 10.101.3.142 | 10.101.3.142 | 4          | HTTP                    | 50    | 2            | 0.74     | 37   | 0               |
| WinServ6     | 10.101.3.116 | 0          | NetBIOS Session Service | 10    | Unreachable  | 0        | 0    | 0               |
| 10.101.3.174 | 10.101.3.174 | 4          | HTTP                    | 50    | 2            | 0.74     | 37   | 0               |
| 10.101.3.132 | 10.101.3.132 | 0          | ssh                     | 20    | Unreachable  | 0        | 0    | 0               |
| 10.101.3.231 | 10.101.3.231 | 4          | HTTP                    | 50    | 2            | 0.74     | 37   | 0               |
| 10.101.3.126 | 10.101.3.126 | 3          | POP3                    | 10    | 2            | 0.77     | 8    | 0               |
| WinServ9     | 10.101.3.121 | 60         | ssh                     | 20    | 2            | 0.98     | 20   | 0               |
| 10.101.3.161 | 10.101.3.161 | 9          | ssh                     | 20    | 2            | 0.98     | 20   | 0               |
| WinServ2     | 10.101.3.113 | 11         | SMTP                    | 60    | 2            | 0.93     | 56   | 0               |

# Security Intelligence Center – Security Impact Query

Security Intelligence Center - 192.168.83.207

Source: Internet  
Destination: Campus\_dist\_1\_ios subnets

Path Status: This path is currently **BLOCKED**

Vulnerabilities on the Destination:  
Permitting this access exposes 55 vulnerabilities.  
75 hosts are exposed in the destination.  
5 of the exposed hosts have leapfrog vulnerabilities.

Downstream Impact:  
Source: 10.101.3.124, 10.101.3.142, 10... Destination: All Trusted Subnets  
761 hosts would be reachable via leapfrog vulnerabilities.

Exposed Hosts with Leapfrog Vulnerabilities - 192.168.83.207

Table shows hosts with leapfrog vulnerabilities that would be exposed by the query-defined access

| Name         | IP Address   | Vulnerabil... | Primary Service | Value | Attack Depth | Exposure | Risk | Downstream Risk |
|--------------|--------------|---------------|-----------------|-------|--------------|----------|------|-----------------|
| 10.101.3.158 | 10.101.3.158 | 4             | HTTP            | 50    | 2            | 0.74     | 37   | 0               |
| 10.101.3.124 | 10.101.3.124 | 4             | HTTP            | 50    | 2            | 0.74     | 37   | 0               |
| 10.101.3.142 | 10.101.3.142 | 4             | HTTP            | 50    | 2            | 0.74     | 37   | 0               |
| 10.101.3.174 | 10.101.3.174 | 4             | HTTP            | 50    | 2            | 0.74     | 37   | 0               |
| 10.101.3.231 | 10.101.3.231 | 4             | HTTP            | 50    | 2            | 0.74     | 37   | 0               |

Client 122 M of 968 M  
Server 2,848 M of 3,944 M

Leapfrog Attack (踏み台攻撃)が可能なホストリスト