

NS156

# 最新アップデート: ネットワークとセキュリティの 可視化を強化

---

ヴィエムウェア株式会社  
ソリューションビジネス本部  
スタッフシステムズエンジニア 高田 和美

#vforumjp

vmware®



POSSIBLE  
BEGINS  
WITH YOU

# 免責事項

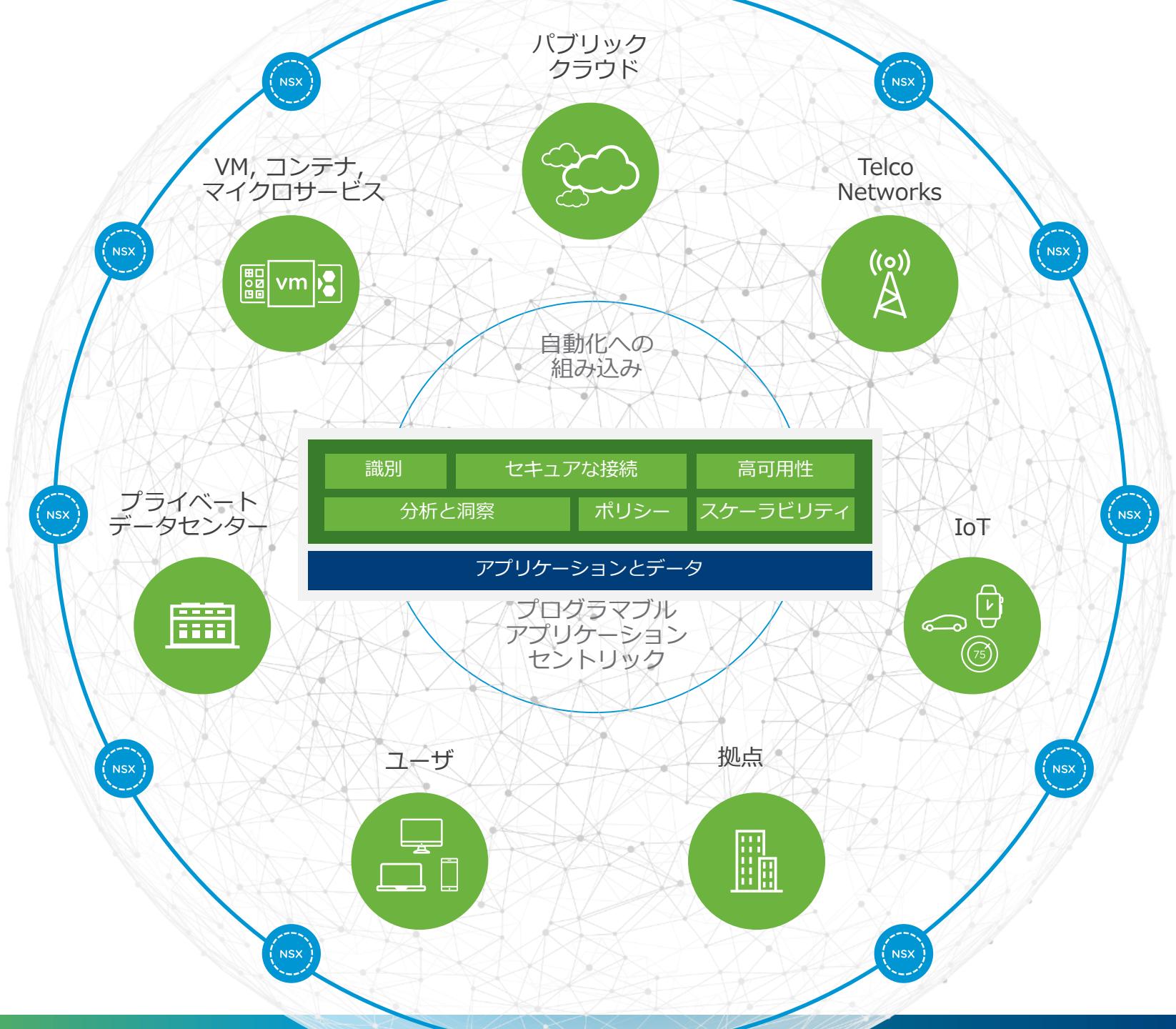
- このセッションには、現在開発中の製品/サービスの機能が含まれている場合があります。
- 新しいテクノロジーに関するこのセッションおよび概要は、VMware が市販の製品/サービスにこれらの機能を搭載することを約束するものではありません。
- 機能は変更される場合があるため、いかなる種類の契約書、受注書、または販売契約書に記述してはなりません。
- 技術的な問題および市場の需要により、最終的に出荷される製品/サービスでは機能が変わる場合があります。
- ここで検討されているまたは提示されている新しいテクノロジーまたは機能の価格およびパッケージは、決定されたものではありません。

# Agenda

1. VMware vRealize Network Insight™(vRNI) をお勧めしたい理由
2. 360 度の可視化
3. トラフィック / フロー分析
4. 問題の発見と解決
5. セキュリティ計画と運用
6. 最新情報

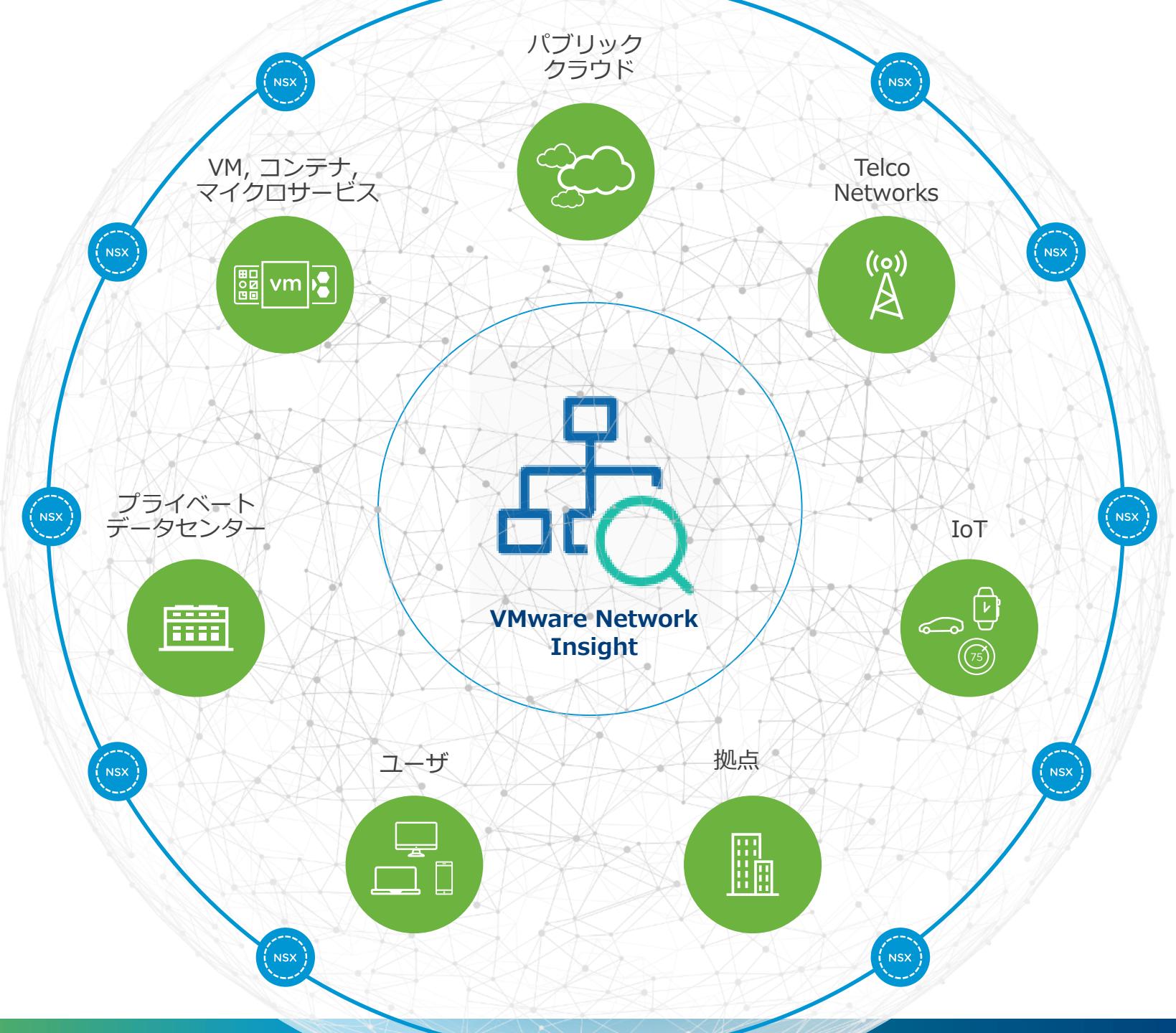
# Virtual Cloud Networking

接続 & 保護  
あらゆる環境にわたって  
あらゆるワークロードへ



# vRealize Network Insight

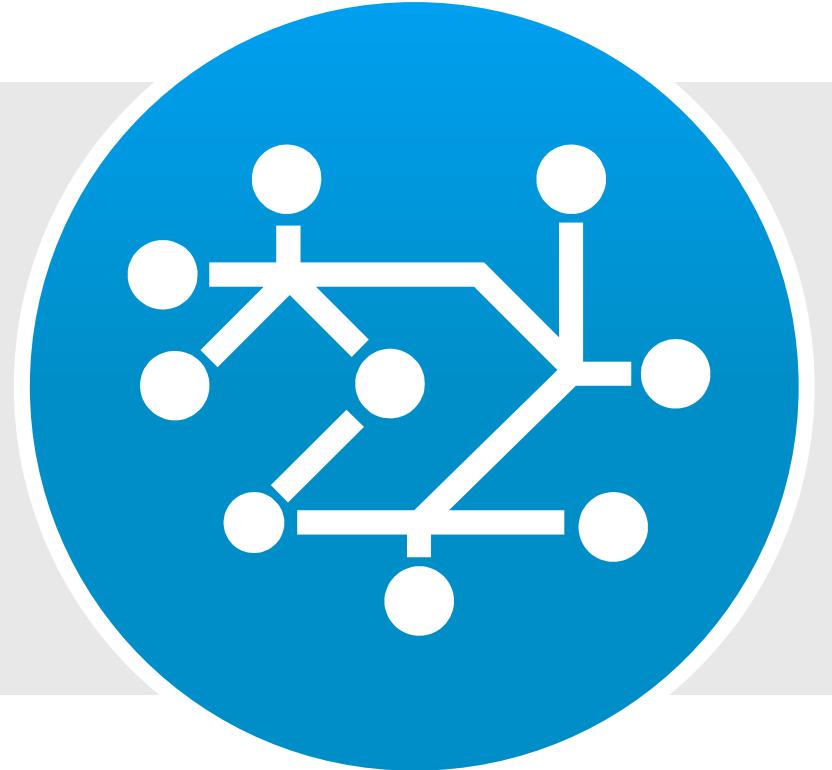
Virtual Cloud Networking へ  
セキュリティ計画 &  
ネットワーク可視化



# vRealize Network Insight (vRNI) をお勧めしたい理由

Why vRNI?

# ネットワークを知る!



# 従来のネットワークツールの課題



ダイナミックな  
ネットワーク  
インフラへの対応



Software-Defined  
Data Center や  
マルチ / ハイブリッド  
クラウド環境に  
わたる可視化の欠如



別々のチーム内で  
利用可能な  
人やツールの不足

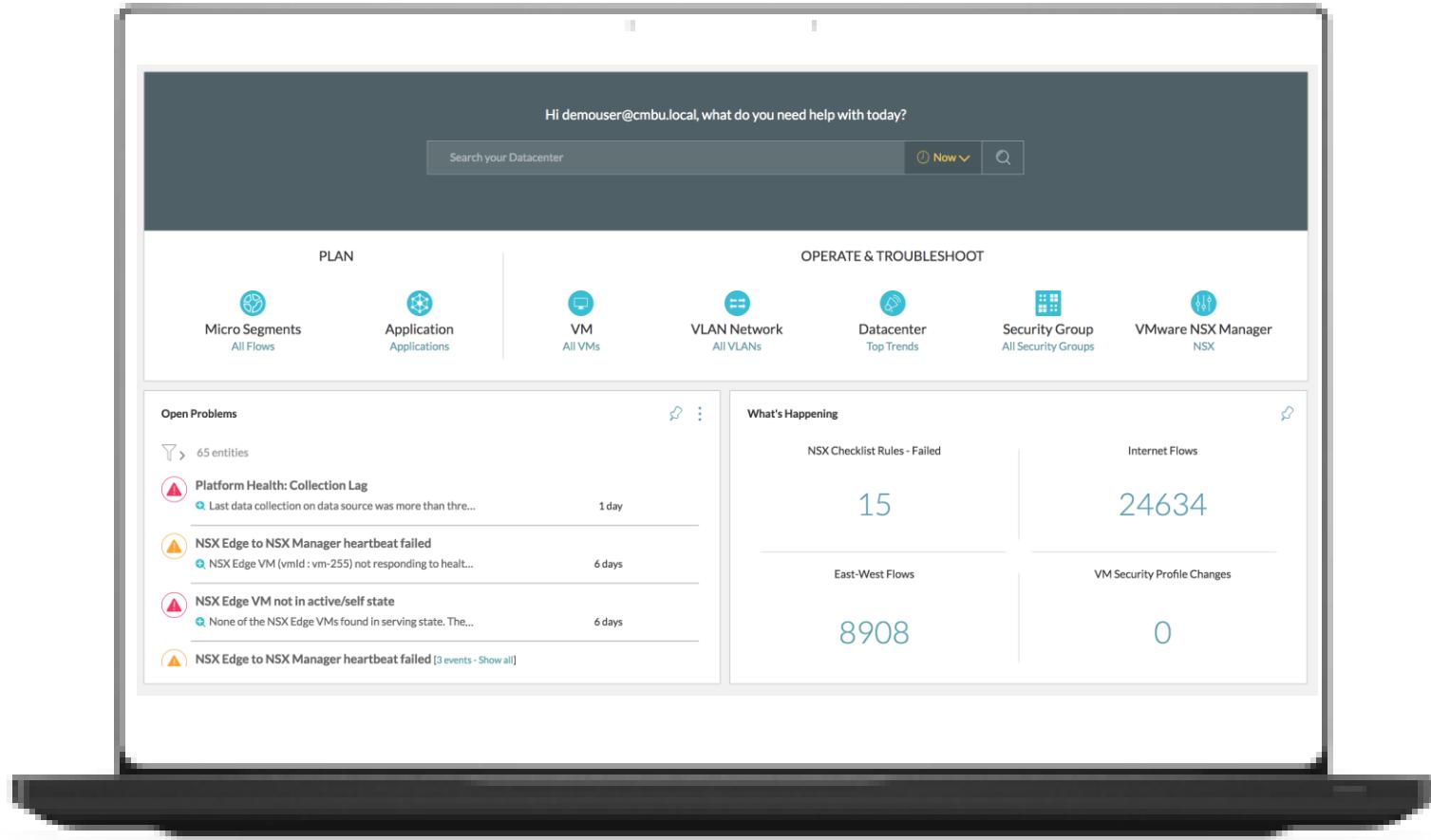
# vRealize Network Insight がソリューションに 物理と仮想のネットワーク間で統合された運用の視点



# vRealize Network Insight ユーザーインターフェース

全体のインフラをまるごと俯瞰

- vRNI のマイクロセグメンテーションルールの推奨を使ってセキュリティ計画
- 仮想と物理のインフラにわたるネットワークとセキュリティのトラブルシューティング
- ベストプラクティスチェックリストを含む NSX 展開の管理とスケール



# 360 度の可視化

# 仮想マシンパス トポロジー (1)

## 詳細分析

可視化の集中

フル ネットワーク  
トポロジマッピング  
(仮想から物理)

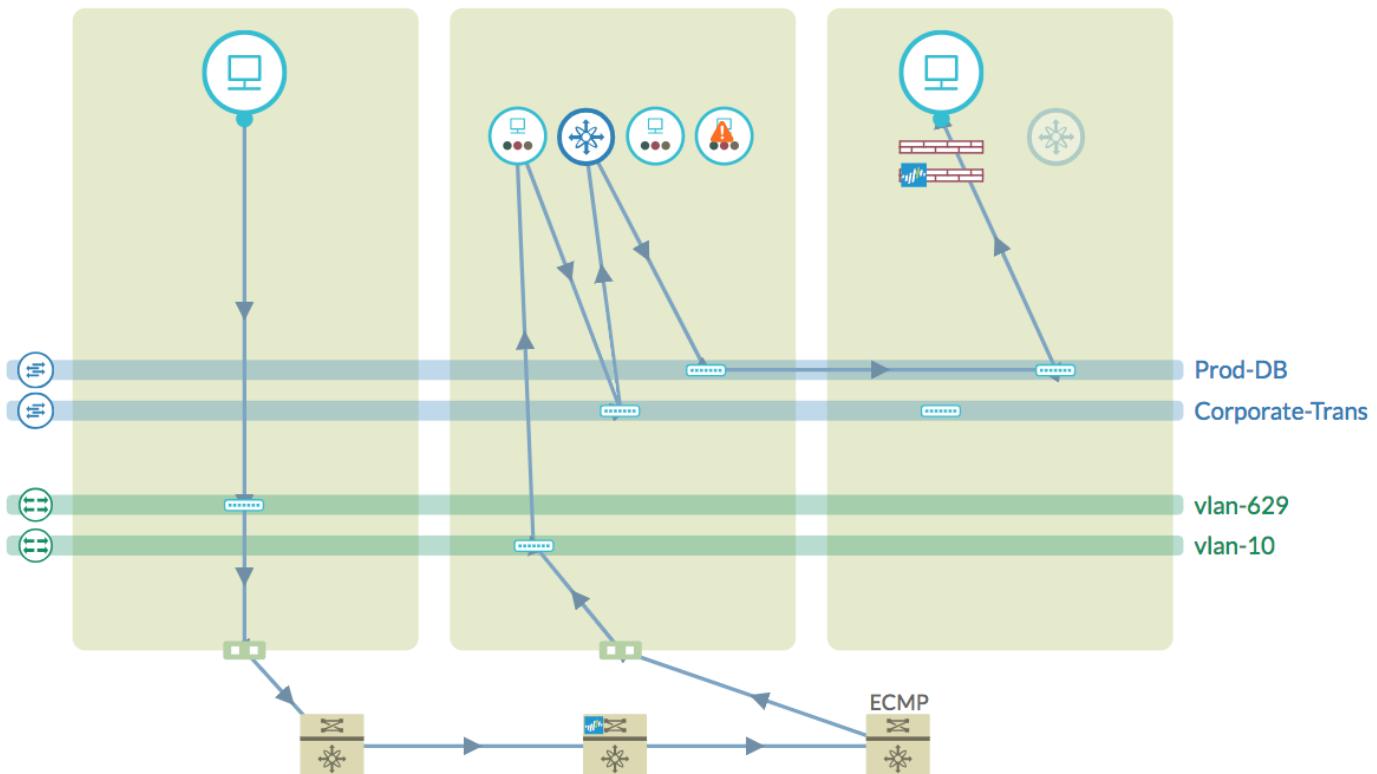
VM Path Topology i

Client  
DBAdmin-VM1  
10.46.1.25

Request

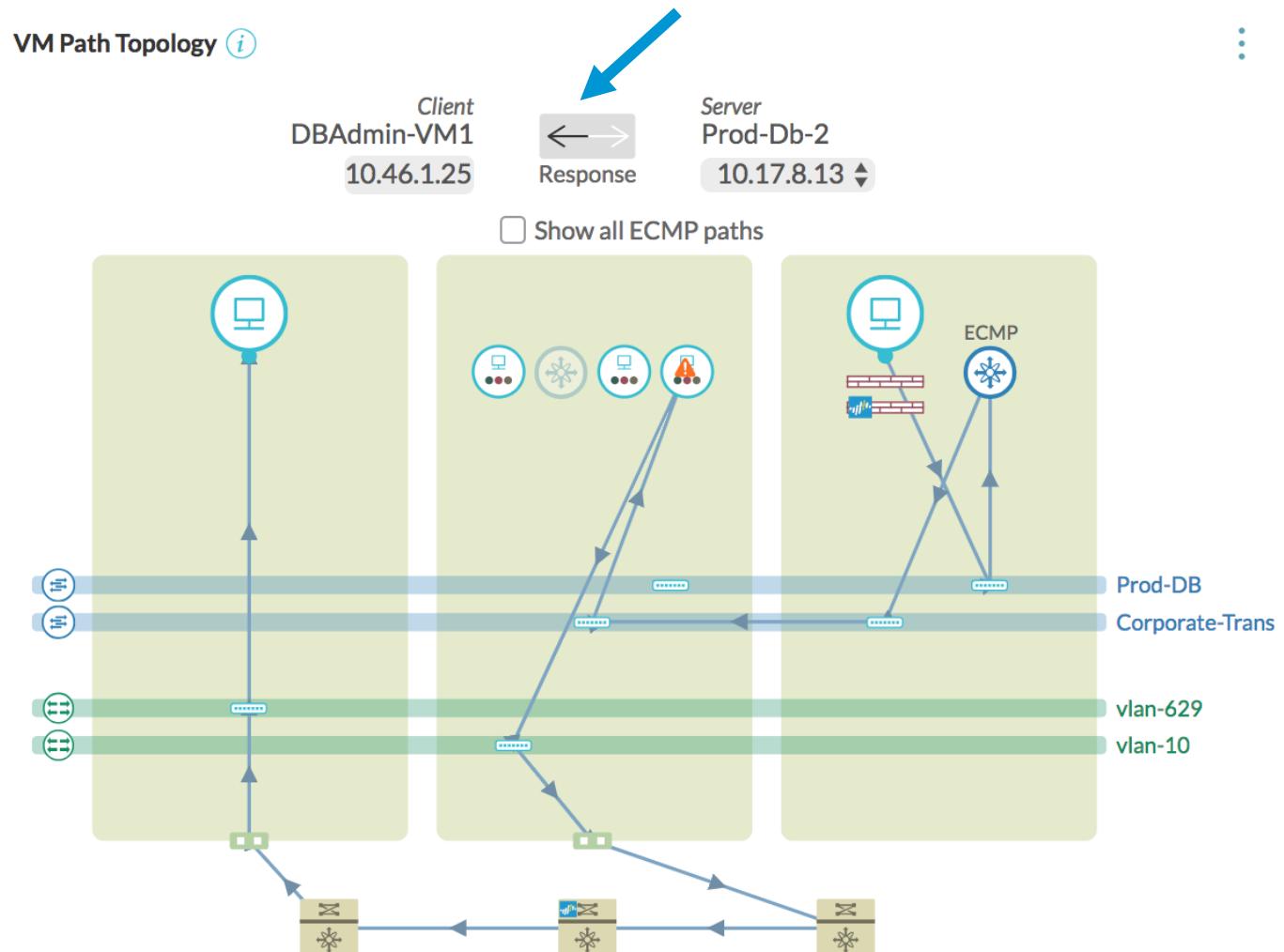
Server  
Prod-Db-2  
10.17.8.13

Show all ECMP paths



# 仮想マシンパス トポロジー (2)

方向の切り替えは簡単



方向はワンクリックで切り替え

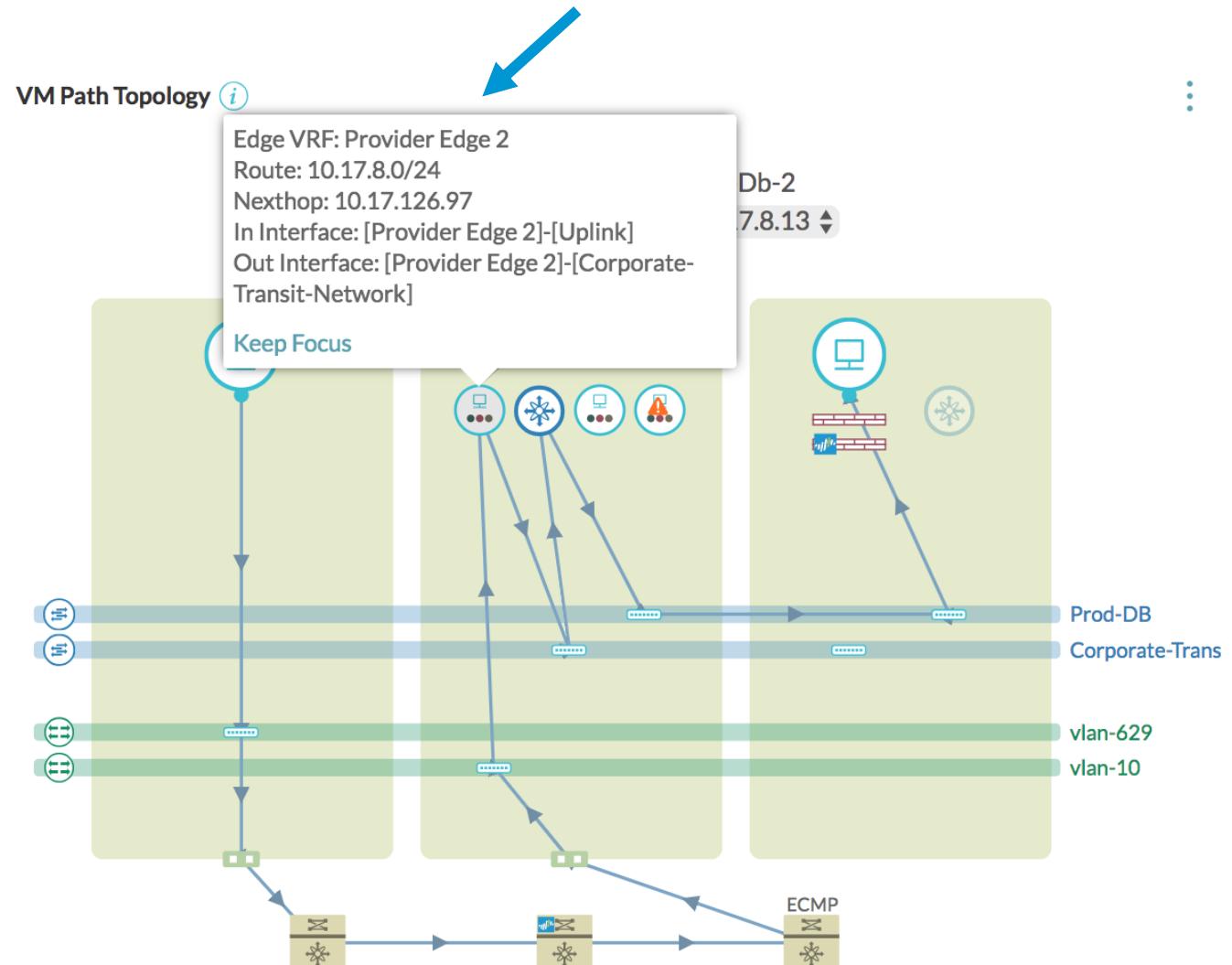
アクティブなパスのその時点の分析

# 仮想マシンパス トポロジー (3)

Edge 設定表示も簡単

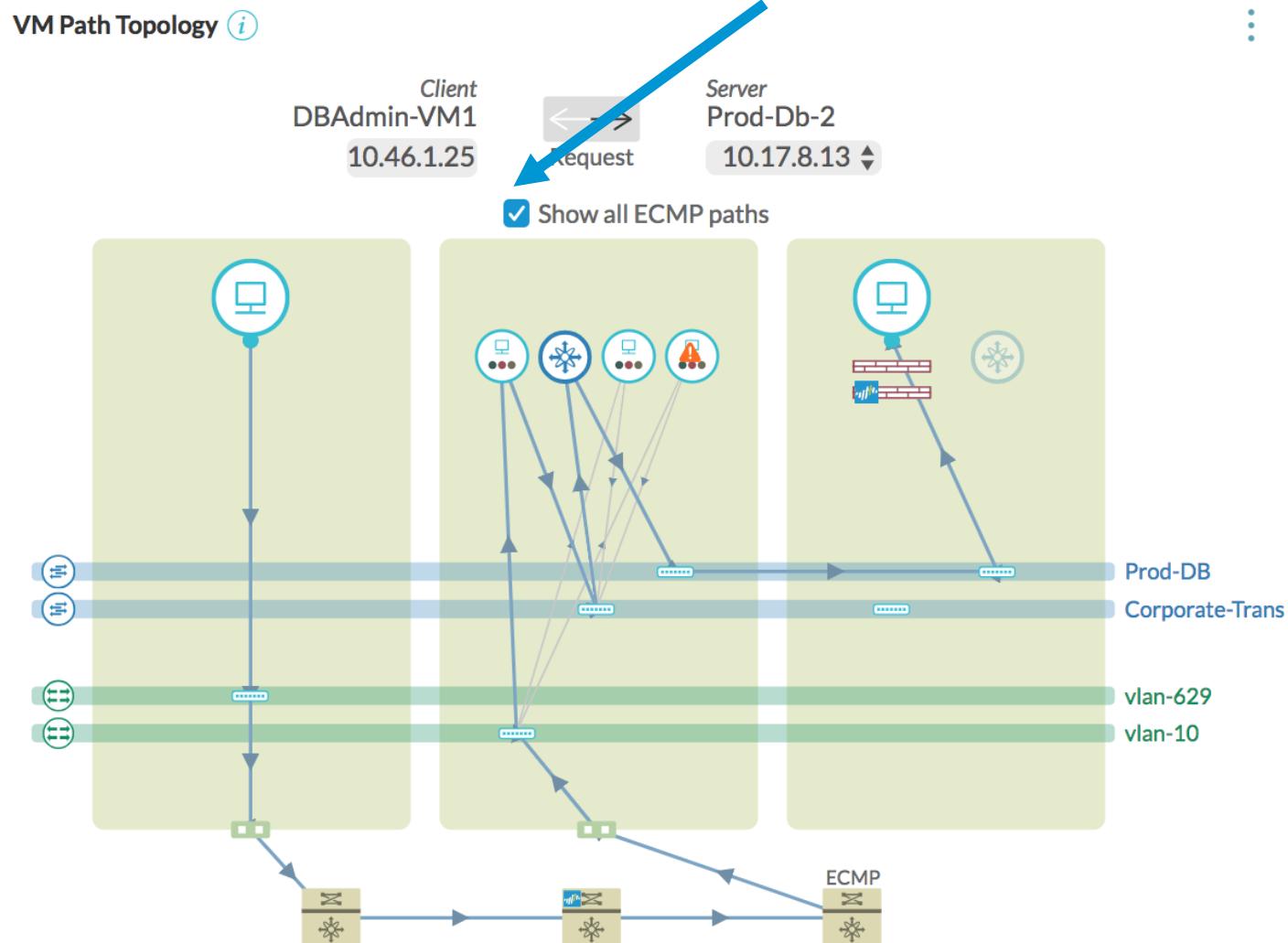
エンティティ設定の  
表示

1 つの図上で確認  
しながらトラブル  
シューティング



# 仮想マシンパス トポロジー (4)

## ECMP パスの詳細



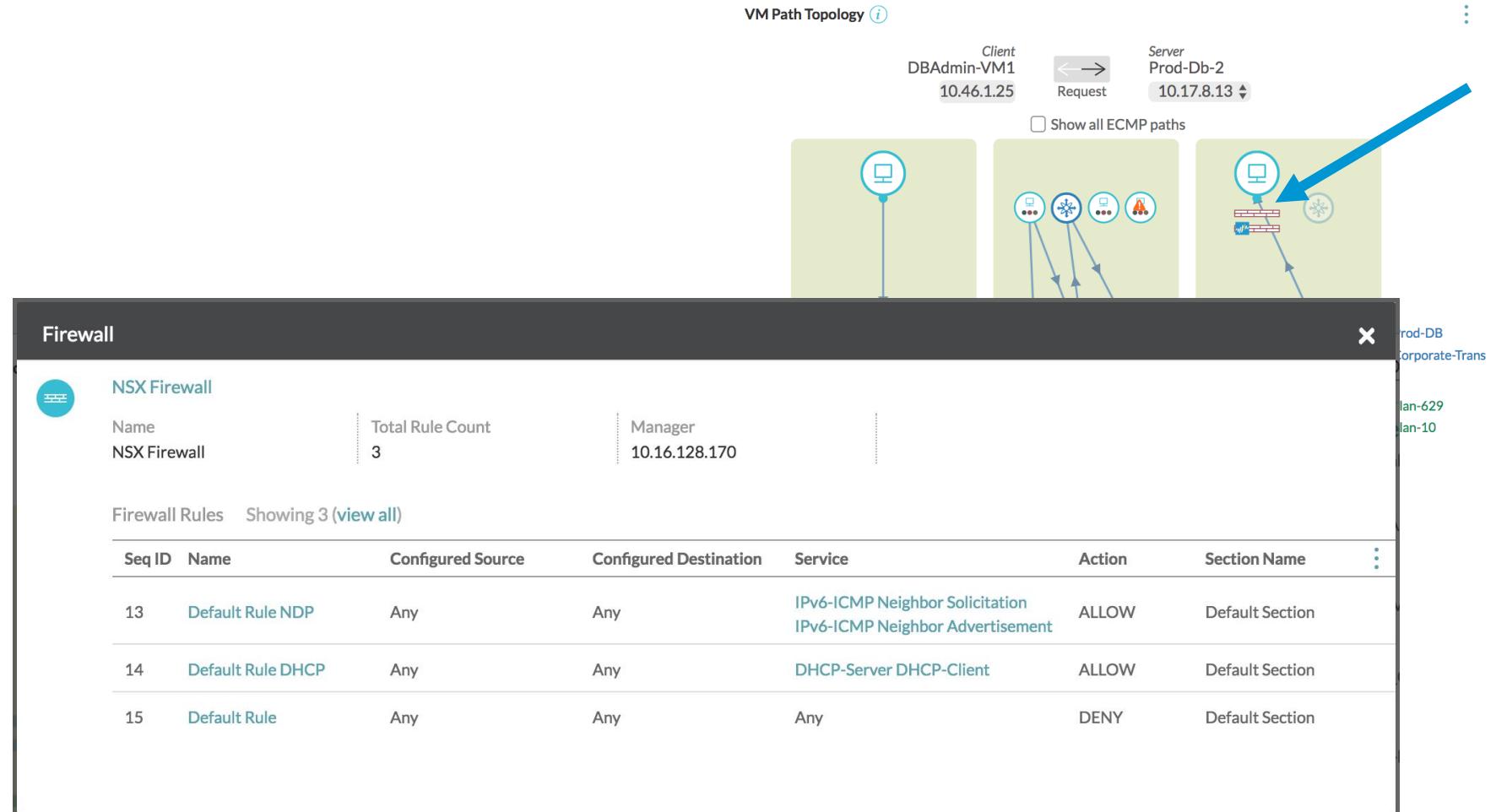
ECMP 設定全体を見るときは “Show all ECMP paths” にチェックするだけ

# 仮想マシン パス トポロジー (5)

## 仮想マシン 分散ファイアウォールの設定

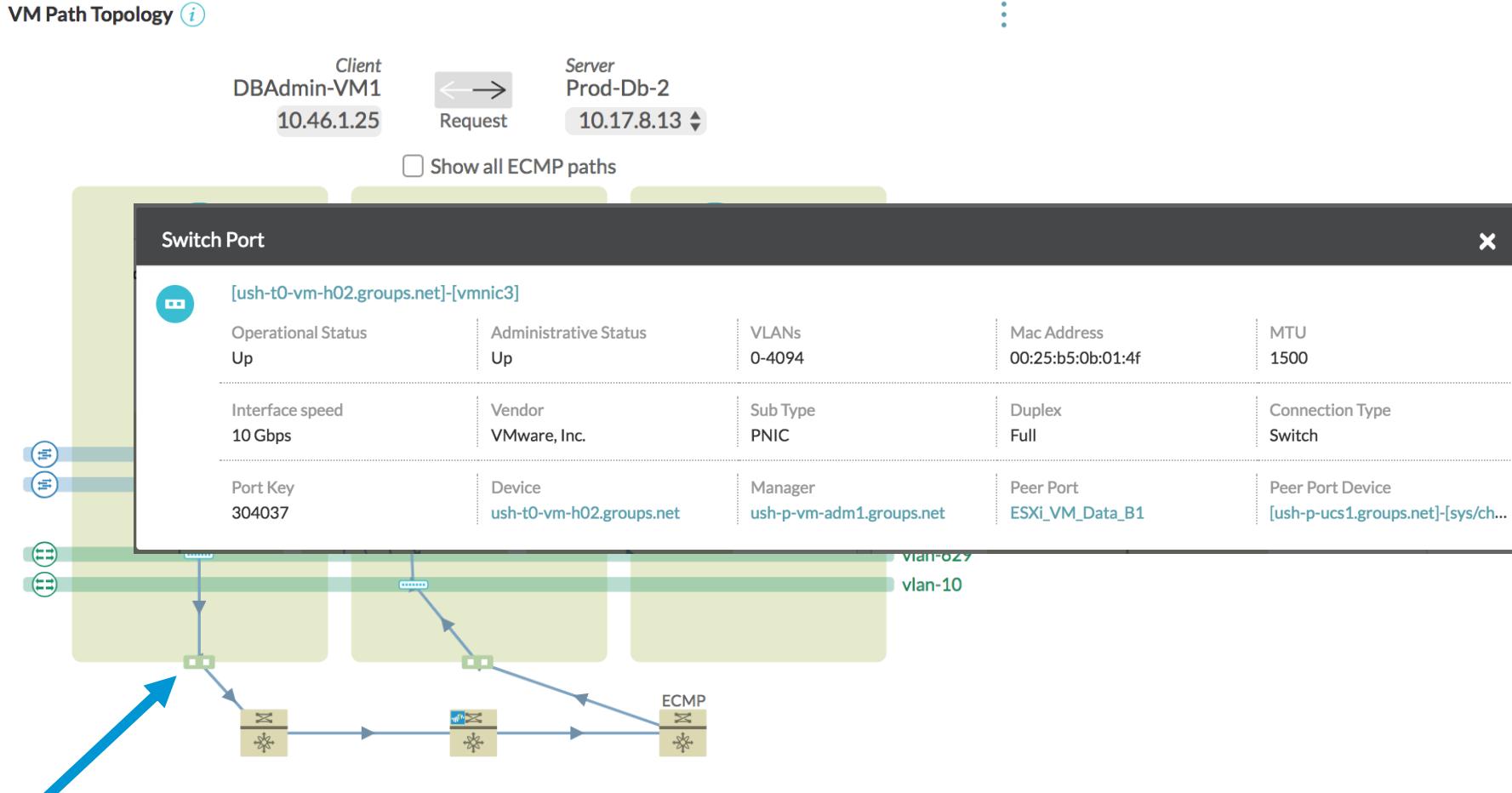
分散ファイアウォー  
ル設定の表示

サードパーティ製も  
統合されている表示



# ホストレベルの詳細

## ホストのネットワーク設定



ホスト設定の確認と  
トラブルシューティ  
ング

# 物理コンポーネントの詳細

## 仮想と物理の設定

物理ネットワーク  
ベンダーの表示も統  
合

最新サポート製品:  
<https://docs.vmware.com/en/VMware-vRealize-Network-Insight/3.9/com.vmware.vrni.install.doc/GUID-4BA21C7A-18FD-4411-BFAC-CADEF0050D76.html>

VRF					
10.254.146.129-default					
Number of Routes 53	Number of Router Interfaces 11	MTUs 9214	Manager 10.254.146.129	Router 10.254.146.129	
Vendor Arista	Type DCS-7050TX-48-R	Serial JPE14483496	Scope Global	Nat Global	
Nat Enabled No	Default Gateway Routers pan-core-vr	Gateway Routers Provider Edge 1 [3 more]	Gateway IP 10.16.252.1 [3 more]		
Routing Table Showing 4 of 53					
Network	Next Hop	Protocol	Interface		
0.0.0.0/0	10.20.1.1	B E	—		
10.16.128.128/26	—	direct	Vlan100		
10.16.136.128/26	—	direct	Vlan110		
10.16.144.128/26	—	direct	Vlan120		
Router Interfaces Showing 4 of 11					
Interface	IPAddress	Network	Operational Status	MTU	Interface speed
Vlan130	10.16.152.188,10.16.152.190	10.16.152.128/26	UP	9214	—
Vlan4094	10.16.254.33	10.16.254.32/30	UP	9214	—
Vlan100	10.16.128.190,10.16.128.188	10.16.128.128/26	UP	9214	—
Vlan110	10.16.136.190,10.16.136.188	10.16.136.128/26	UP	9214	—

# パートナーソリューションの詳細

## パートナー統合のサポート

VRF

pan-core-vr	Number of Routes 9	Number of Router Interfaces 3	Router 10.16.21.2	Vendor Palo Alto Networks	Type PA-5060
Version 6.0.9	Serial 09683482408	Scope Global	Nat Global	Nat Enabled No	
Gateway Routers <a href="#">10.254.146.129-default</a> [1 more]	Gateway IP 10.20.1.2 [2 more]				

Routing Table Showing 4 of 9

Network	Next Hop	Protocol	Interface
0.0.0.0/0	10.50.1.100	dynamic	ethernet1/2.3030
10.16.0.0/16	10.20.1.2	dynamic	ethernet1/1.1025
10.17.0.0/16	10.20.1.2	dynamic	ethernet1/1.1025
10.20.1.0/30	-	direct	ethernet1/1.1025

FirewallTable Showing 2 ([view all](#))

Seq ID	Name	Configured Source	Configured Destination	Service	Action	Section Name	NSX Manager	Manager	Scope	Rule ID	Direction
1	Address_Admin to Address_Prod Rule	Address_Admin	Address_Prod	Any	ALLOW	-	-	10.16.128.200	-	-	-
4	ANY to ANY Deny Rule	Any	Any	Any	DENY	-	-	10.16.128.200	-	-	-

Router Interfaces Showing 3 ([view all](#))

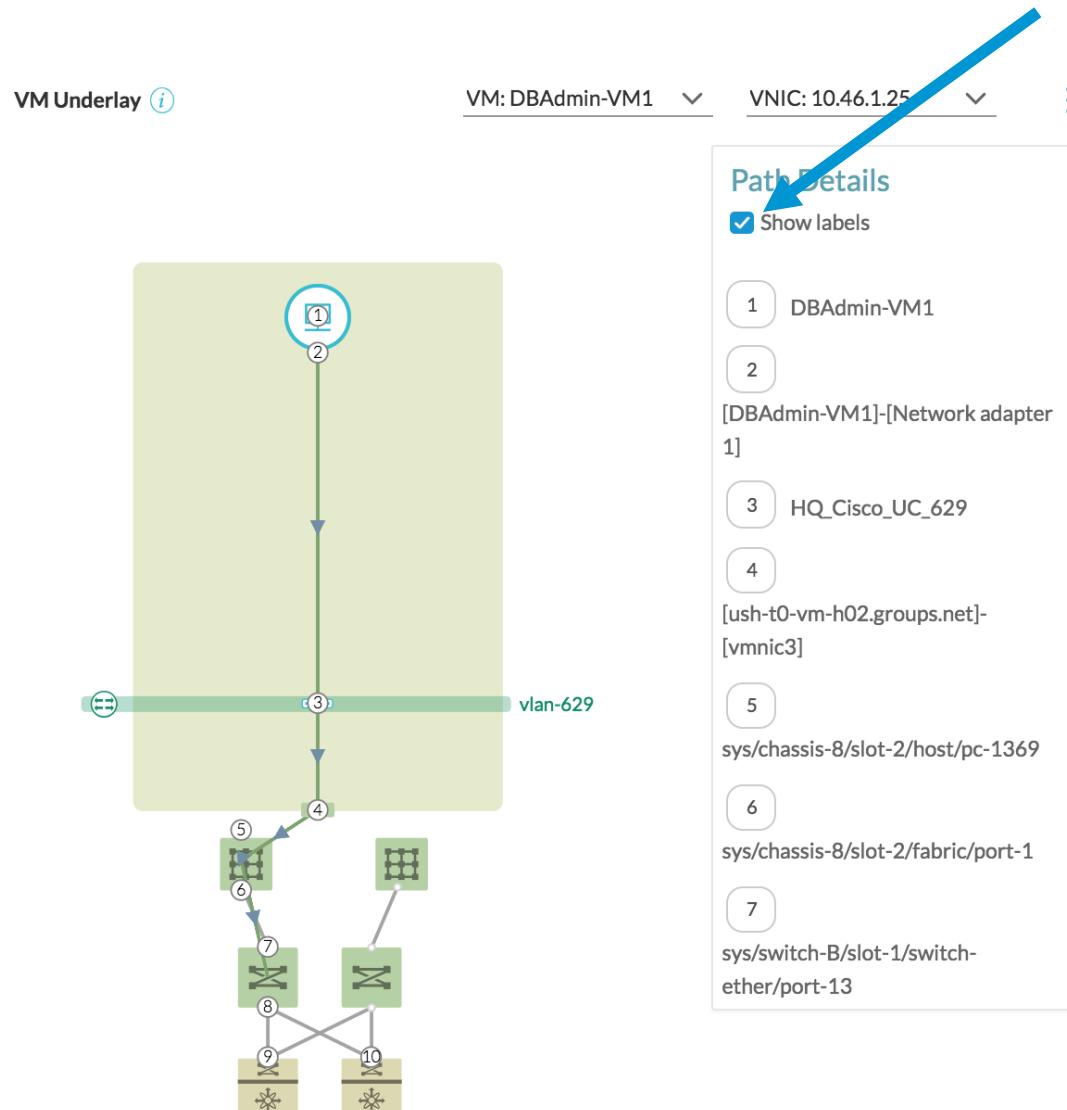
Interface	IPAddress	Network	Operational Status	MTU	Interface speed
ethernet1/2.3030	10.50.1.1	10.50.1.0/24	UP	-	-

单一画面で見る

# 仮想マシン アンダーレイ (1)

## 仮想マシンの具体的なパス詳細

“Show labels”に  
チェックすると自動  
的に番号が付与され  
て、それが何か  
わかる



# 仮想マシン アンダーレイ (2)

## 仮想マシンの設定を見る

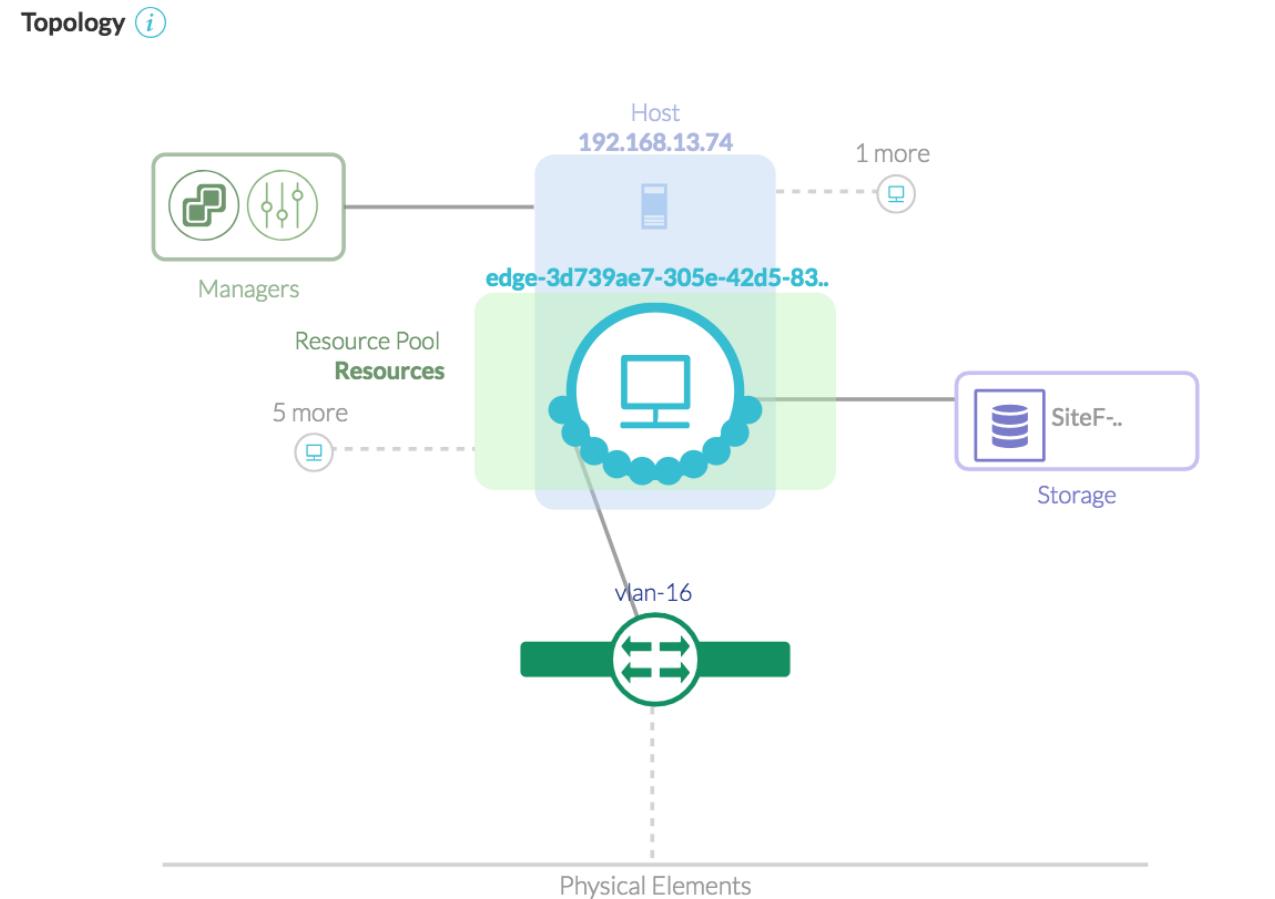
VM				
 DBAdmin-VM1				X
VLANs 629	IP Address 10.46.1.25	Disks DBAdmin-VM1-Hard disk 1	Datastore HQ-T0-03-VPLEX1 [1 more]	Host ush-t0-vm-h02.groups.net
Cluster ROCKY Tier 0_9	Version vmx-08	Datacenter Hercules	Manager ush-p-vm-adm1.groups.net	Power State On
Connection State Connected	CPU Cores 1	Memory (GB) 4	Firewall Status Unknown	VNIC Count 1
Def Gateway 10.46.1.1	Default Gateway Router 10.45.0.253-default	Default Gateway Router Inte... Vlan629	Network Address 10.46.1.0/26	Disconnected VNIC Count 0
OS Red Hat Enterprise Linux 6 (6...)	Resource Pool Resources	DVS dvSwitch0 - Data	DVPG HQ_Cisco_UC_629	FQDN ush-d-uni-cnx1

1 クリックだけで仮想マシンの詳細情報が見える

# 仮想エンティティの詳細

vRNI を離れる必要なく仮想マシンや NSX Edge の詳細表示

vSphere と NSX  
エンティティ関連  
リソースを確認

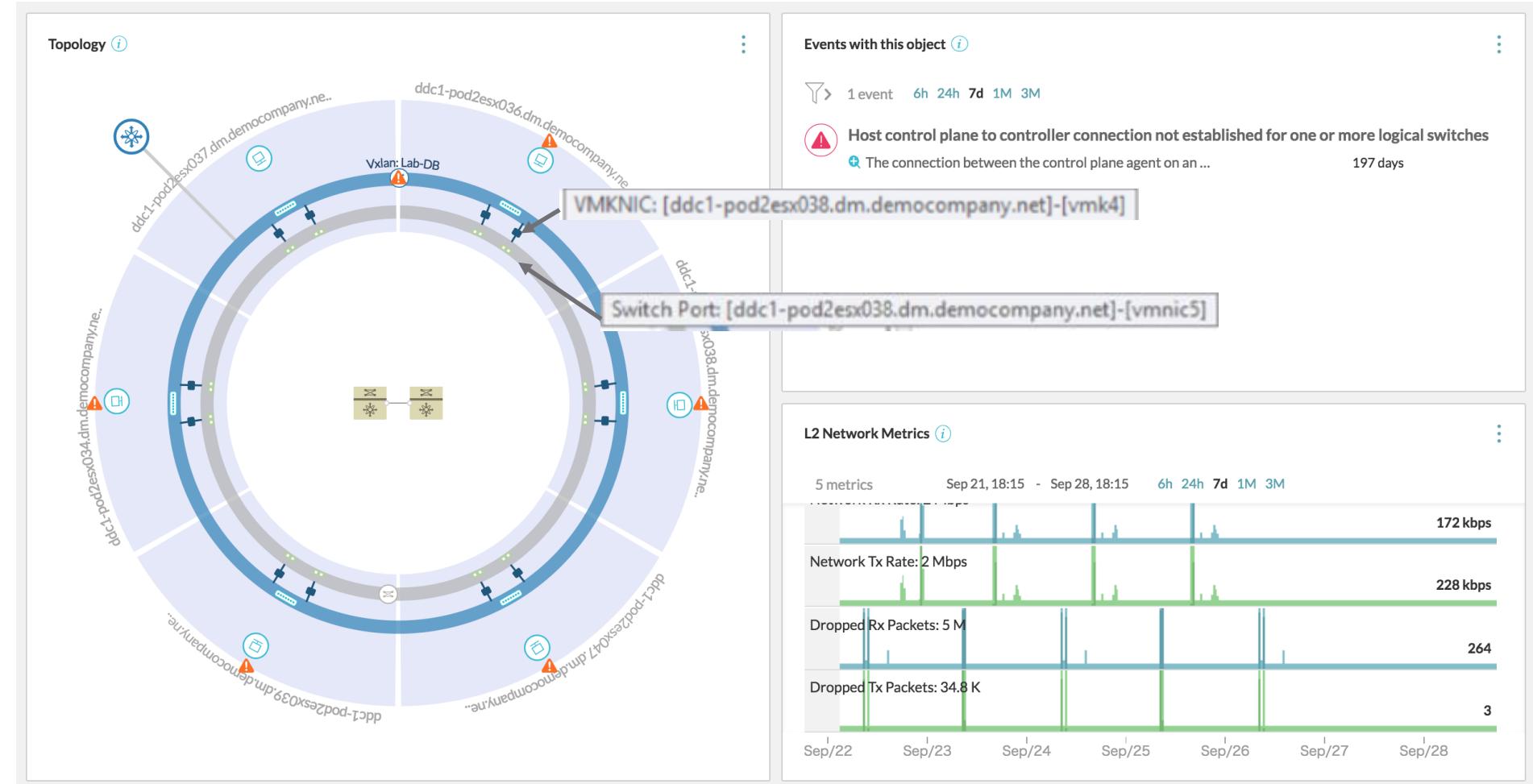


# トラフィック / フロー分析

# トラフィック分析

## トポロジー, エラー, メトリック表示

ネットワーク  
メトリックの中で  
関係性の知見を得る



# トータルなフロー分析

全フロー - 1 つの画面で表示

Micro-Segments i

⋮

Services and Flows for Prod-Web

Services in this group	External Services Accessed	Flows (Incoming and Outgoing)	Recommended Firewall Rules
50	17	575	6

Recommended Firewall Rules

Source	Destination	Services	Protocols	Action
Prod-Web	Prod-Midtier	8080	TCP	ALLOW
Others_Physical	Prod-Web	22 [ssh]	TCP	ALLOW
Prod-Web	Others_Physical	53 [dns]	TCP	ALLOW
Prod-Web	Others_Physical	389 [ldap]	UDP	ALLOW
Prod-Web	Others_Internet	443 [https]	TCP	ALLOW
Others_Internet	Prod-Web	443 [https]	TCP	ALLOW

▶ Destination Port  
▶ Destination Subnet Network  
▶ Bytes \_BYTES\_  
▶ Traffic Rate \_TRAFFIC RATE\_

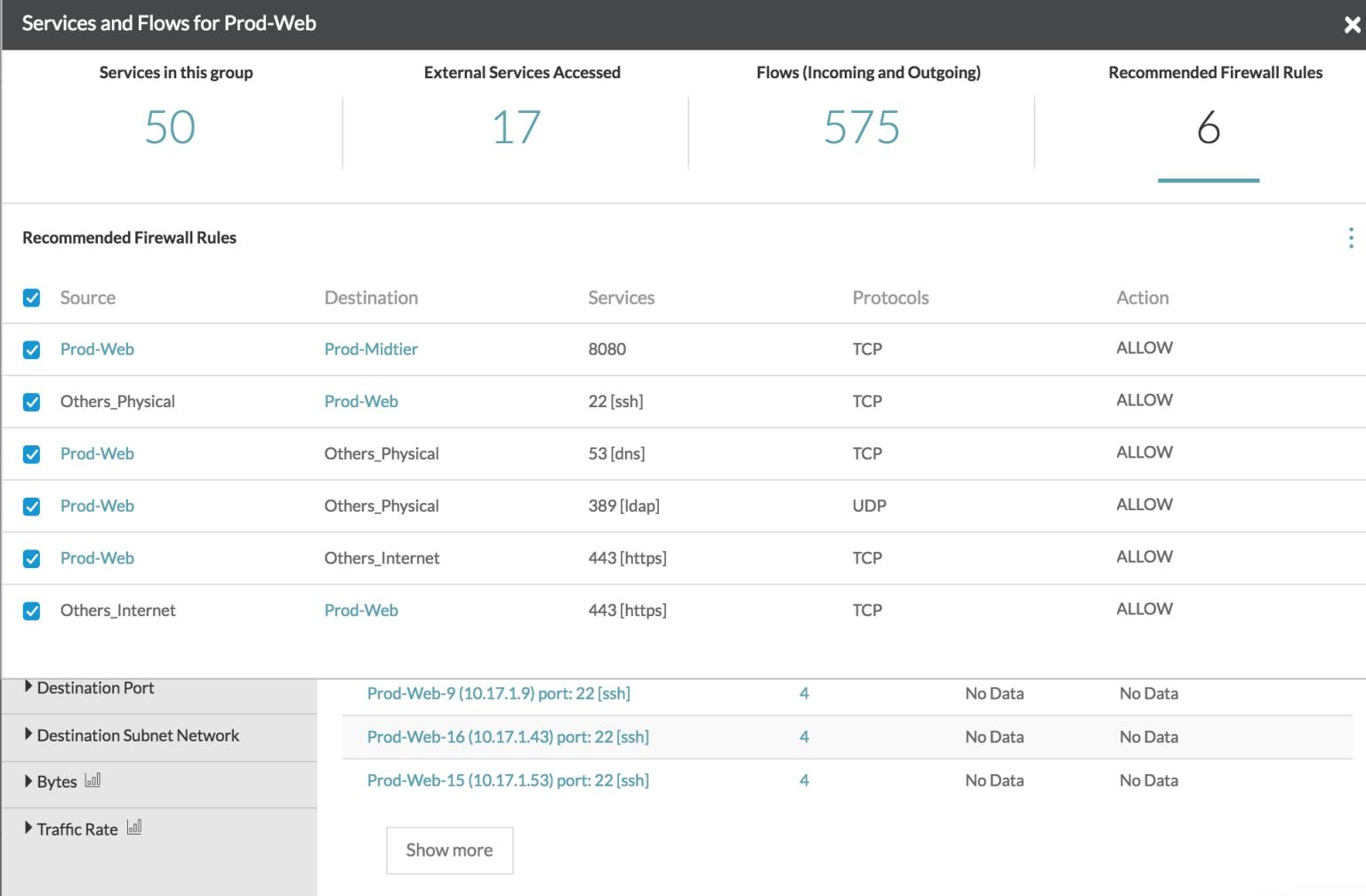
Prod-Web-9 (10.17.1.9) port: 22 [ssh] 4 No Data No Data

Prod-Web-16 (10.17.1.43) port: 22 [ssh] 4 No Data No Data

Prod-Web-15 (10.17.1.53) port: 22 [ssh] 4 No Data No Data

Show more

incoming Bidirectional



仮想と物理のネットワークにわたり可視化と解析でネットワークパフォーマンスと可用性を最適化

リアルなトラフィック分散情報と検知

# 上位通信

## エンティティ間の詳細な分析

タイプごとの上位  
通信



フロー量

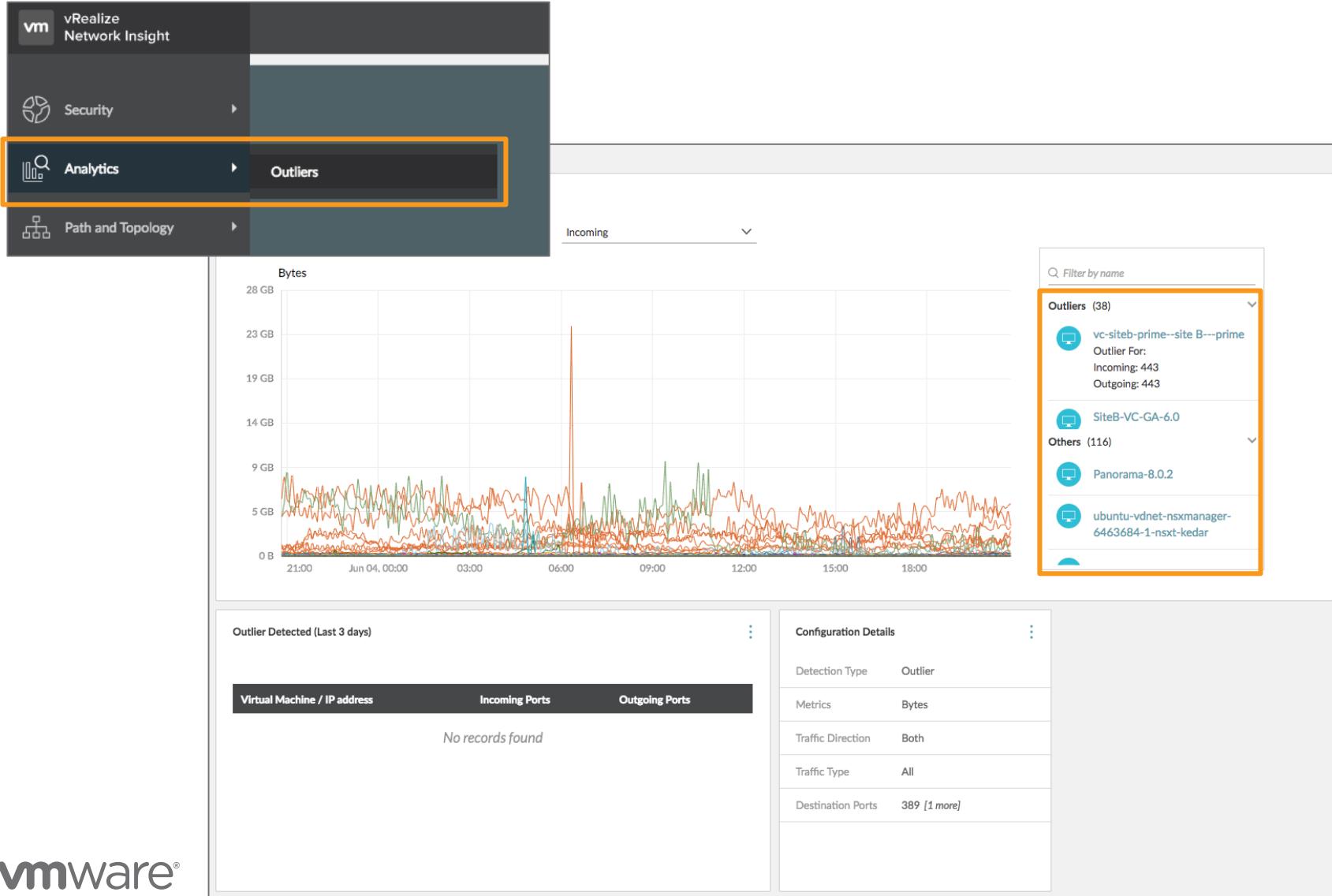
トラフィック  
レート

セッション数

フロー数

# フロー分析

## 異常値の検知



VM と IP アドレスの  
特定のスコープで異  
常値の検知

グループ内の他と異  
なる VM、類似した  
VM 間のネットワー  
クトラフィックのふ  
るまいの違い

ネットワークトラ  
フィック、セッショ  
ン数の量を監視

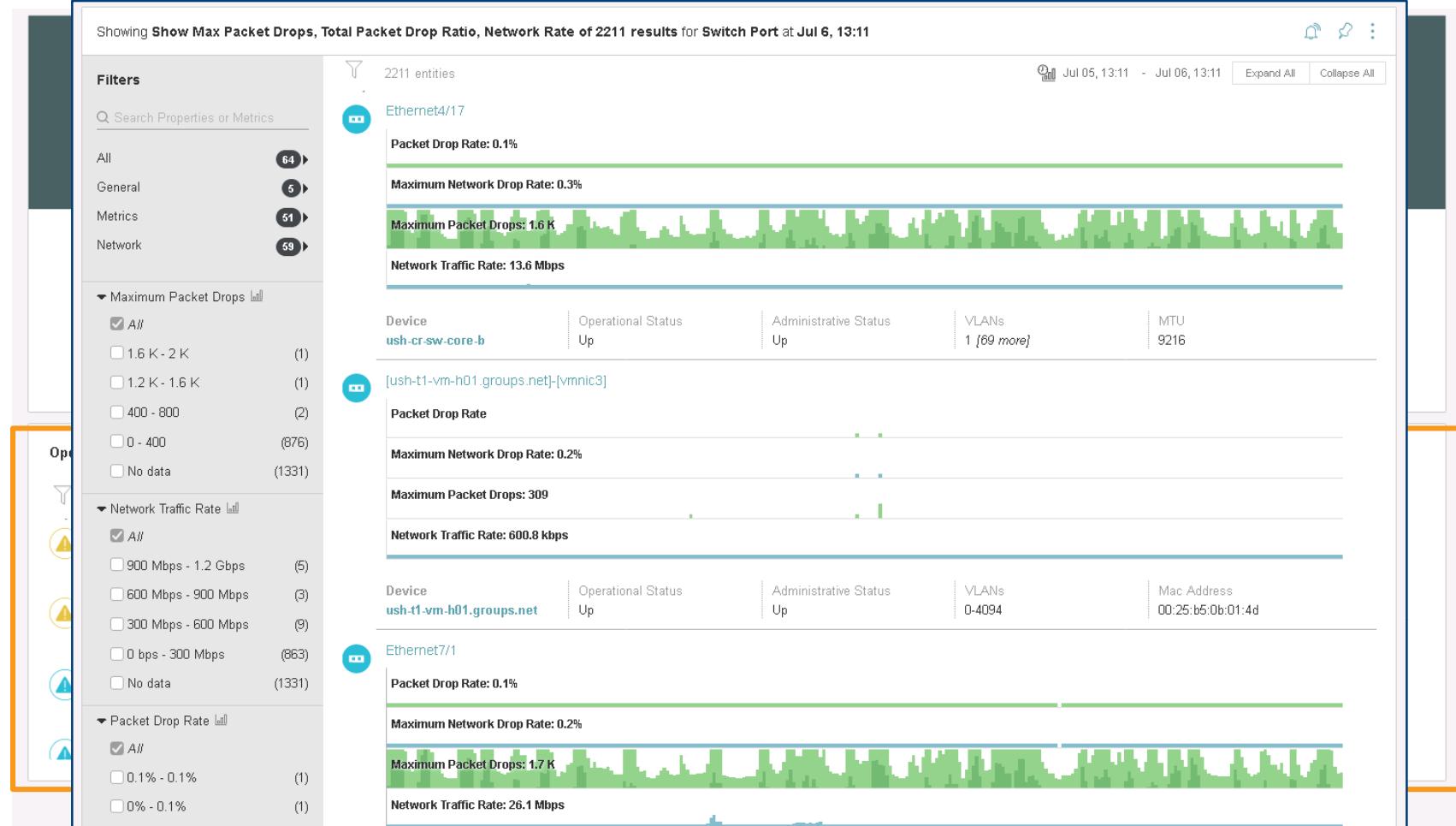
ロードバランサや  
ネットワークのミス  
設定を発見

# 問題の発見と解決

問題はどこにありそうか、解決・改善の方法は？

# エラーを見つける

## 検索のための多くの方法



未解決問題

発生していること

オブジェクトやパス  
トポロジーのための  
わかりやすい検索

# ソリューションを見つける “深掘り”

Hi Administrator, what do you need help with today?

Search Your Data Center

Event

**Service VM's status mismatched between Panorama and NSX Manager**

Mismatch in service appliance information between NSX Manager and Panorama.

Severity: Critical

Manager: 10.16.128.200

Defined By: System

Event Tags: Palo Alto Networks, NetX

Message: NSX Security Fabric Agent Palo Alto Networks NGFW(ddc1-pod2esx040.dm демокомпания.net) has no corresponding Palo Alto device reported by Panorama on host ddc1-pod2esx040.dm демокомпания.net

Panorama: 10.16.128.200

NSX manager: 10.16.128.170

Recommendation 1: Check the state of the Palo Alto NGFW virtual machine and ensure that it is booted properly

Recommendation 2: Confirm network connectivity exists between the Palo Alto NGFW virtual machine and Panorama

Recommendation 3: Confirm network connectivity exists between the Palo Alto NGFW virtual machine and NSX Manager

**Service VM's status mismatched between Panorama and NSX Manager**

Mismatch in service appliance information betwe...

227 days

East-West Flows

VM Security Profile Changes

2463

35

**NSX Fabric Agent not found on Host** [7 events - Show all]

Security Fabric Agent not reported by NSX for a Hos...

227 days

未解決問題

# ソリューションを見つける “深掘り”

NSX Checklist Rules - Failed

Filters

Search Properties or Metrics

All 9 ▶

Event Name

Status

Archived

Severity

Defined By

Manager

Problem Entity

NSX Security

Service Mesh

NSX Firewall

広げる

Distributed firewall rule masked by preceding rule

A distributed firewall rule is masked by one or more preceding rules. This condition may indicate a configuration error, such as a redundant rule.

Severity: Warning

Manager: 10.16.128.170

Defined By: System

Event Tags: Security, Firewall

NSX Firewall Rule: Lab Web to Lab DB - DBService (Rule Id: 1021, Seq #: 12) is masked by rule Lab to Lab Rule (Rule Id: 1010, Seq #: 1)

Seq No	Name	Rule Id	Source	Destination	Service	Action
1	Lab to Lab Rule	1010	Lab	Lab	ANY	ALI
12	Lab Web to Lab DB	1021	Lab_Web	Lab_Db	DBService	DE

Recommendation: Validate the modification was expected. If not planned or expected, configure the required firewall rule(s).

未解決問題

発生していること

# ソリューションを見つける

## “深掘り”



### DLR networks unreachable from NSX Edge or external router

- One or more DLR networks cannot be reached from the uplink interface on the NSX Edge router. This condition suggests either an OSPF configuration error on the Edge-router/DLR or route not configured on uplink router.

**Severity:** Critical

**Manager:** 10.16.128.170

**Defined By:** System

**Event Tags:** Networking, Edge

**Message:** DLR: [LDR-Release](#) networks are not reachable from Router: [Provider Edge 1](#) due to a routing issue.

**Affected Networks:** [Release-Tools](#)

**Recommendation 1:** Check the routes on the router connected to the uplink of the NSX Edge router

**Recommendation 2:** Route to reach the distributed logical router should exist on the router connected to the uplink of the NSX Edge router



### OSPF area ID mismatched between DLR and Edge router

- The OSPF area ID differs on connected router interfaces.

**Severity:** Moderate

**Manager:** 10.16.128.170

**Defined By:** System

**Event Tags:** Networking, Configuration, Edge

**Message:** OSPF Area ID 12 of router: [LDR-Release](#) is absent in router: [Provider Edge 1](#)

**Recommendation:** Configure the same OSPF area ID for the DLR and Edge router interface mapping.

未解決問題

発生していること

オブジェクトやパス  
トポロジーのための  
わかりやすい検索

# 注意が必要なもの、よく見るものは集めてピンボード作成

ピンマークからピン  
ボードを作成

自分専用、他のユー  
ザに共有可能

ピンボードは表示の  
み、表示&更新可能  
のを共有時に指定

システム全体で最大  
500 ピンボード  
(最新。以前は最大  
20)

The screenshot shows the VMware Pinboard interface. At the top, there is a "VM Path Topology" section with two nodes: "Client web-01a" (IP: 10.196.165.69) and "Server app-01a" (IP: 172.16.13.102). A "Request" arrow points from the client to the server. To the right of the topology is a "Pin Options" sidebar with a search bar and a list of recently modified pinboards: "Default Pinboard", "Fitcycle-Big-App\_Monitoring", and "CRM App".

Below the topology is a "Pinboard Library" section. At the bottom of the library is a navigation bar with "My Pinboards" (highlighted with an orange box) and "All Pinboards".

The main area displays a list of pinboards:

Pinboard name	Last modified	Owner	Shared	Actions
Default Pinboard	2 days	Administrator	Not shared	
Fitcycle-Big-App_Monitoring	22 hr	Administrator	Not shared	
CRM App	3 days	Administrator	Not shared	

# セキュリティ計画と運用

# アプリケーションのフローを確認

想定している通信なのか確認

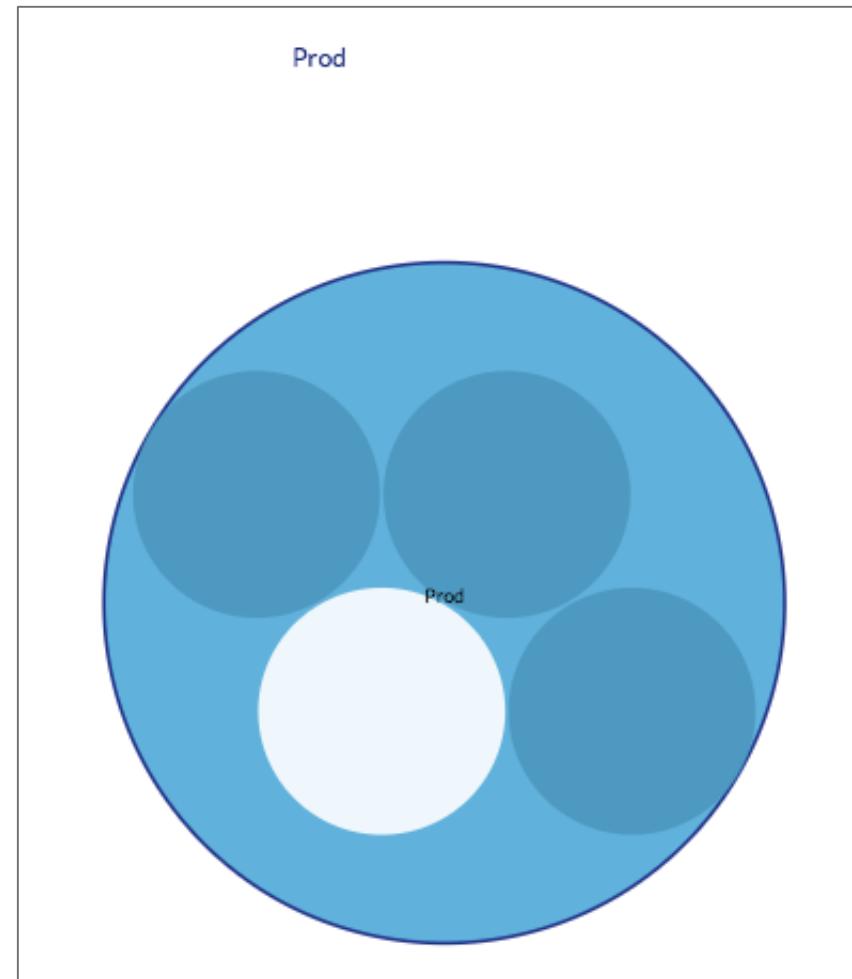
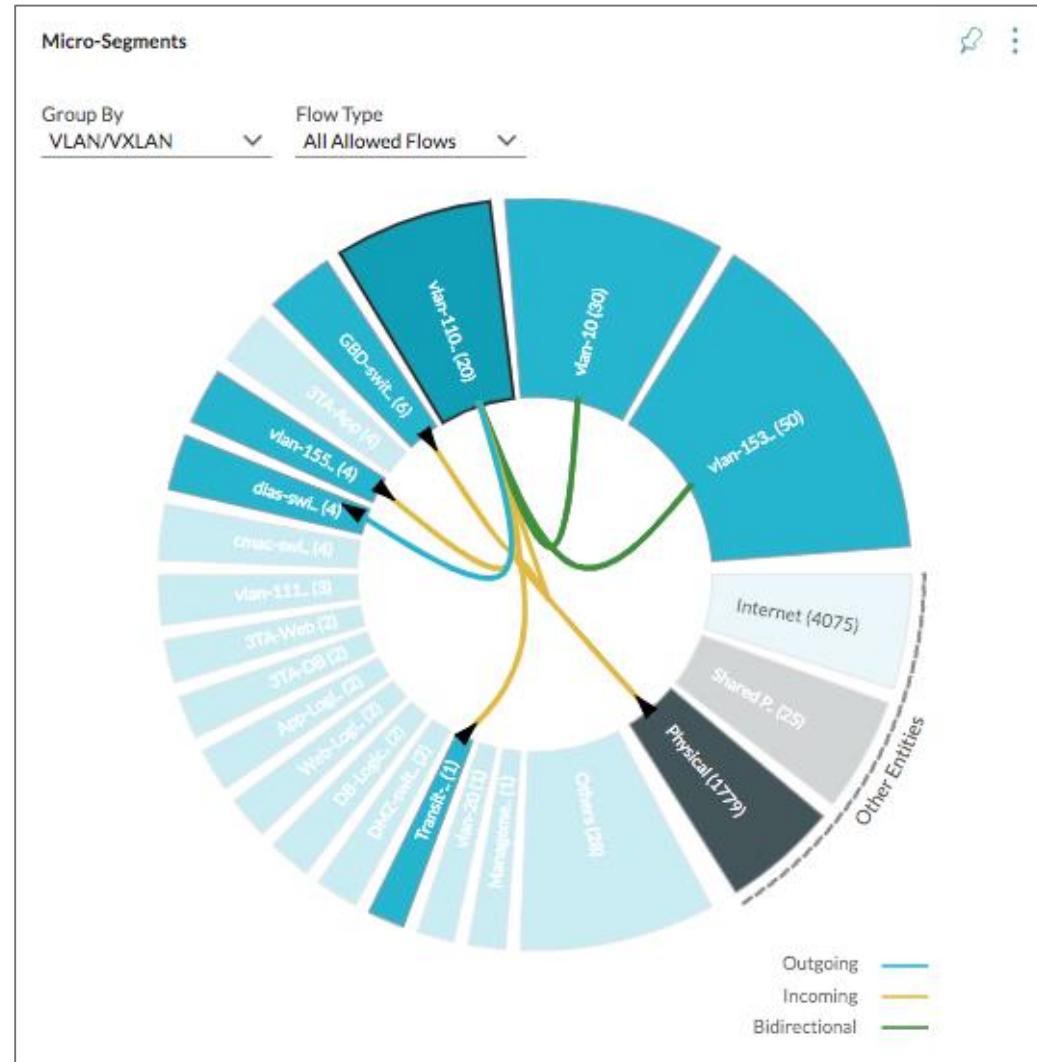
通常のネットワーク  
通信を認識 (アプリ  
ケーションや階層)

推奨のセキュリティ  
ポリシーやファイア  
ウォールルール

現在を正しい状態とし  
て異常 (セキュリティ  
脅威) への対策

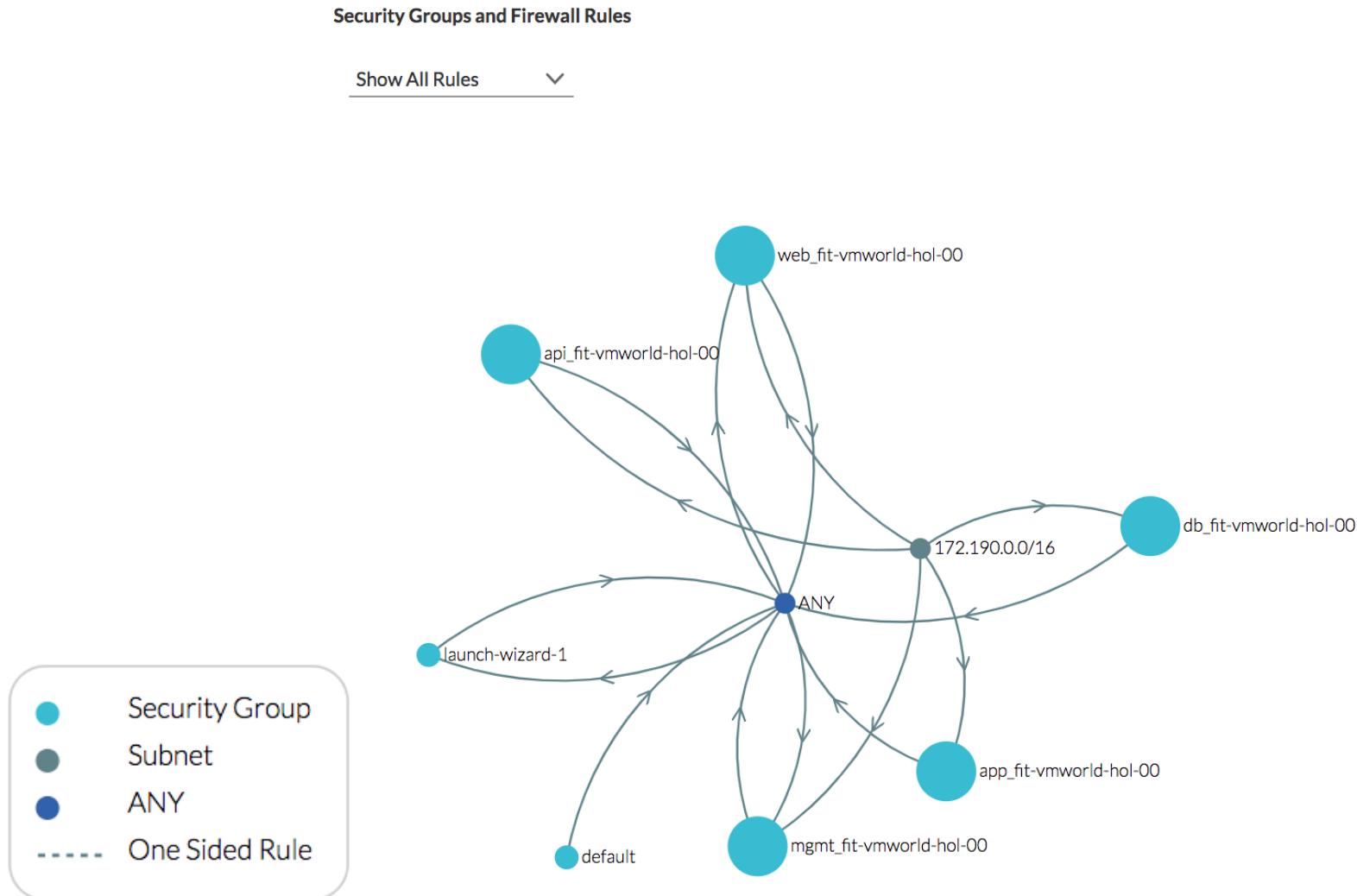
セキュリティグループ  
の関係

メンバーシップ



# アプリケーションのフローを確認

想定している通信をしているのか、AWS でも確認

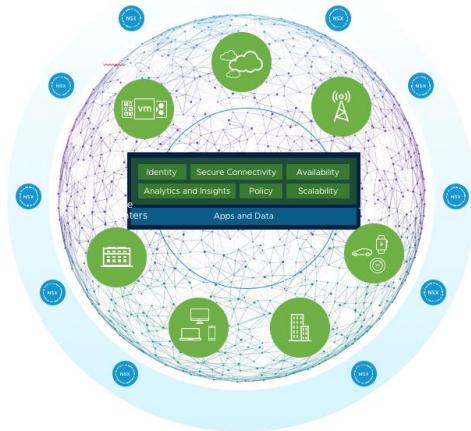


Native AWS のセキュリティグループとファイアウォールルールの確認

# 最新情報

# vRealize Network Insight 最新情報

プライベート、パブリック、ハイブリッドクラウドにわたるアプリケーション中心のセキュリティ計画とネットワークの可視化

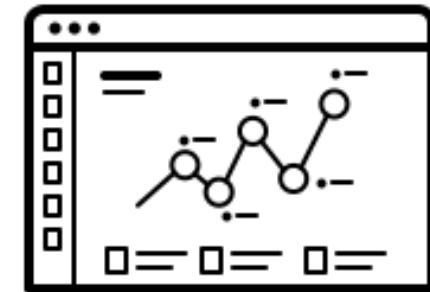
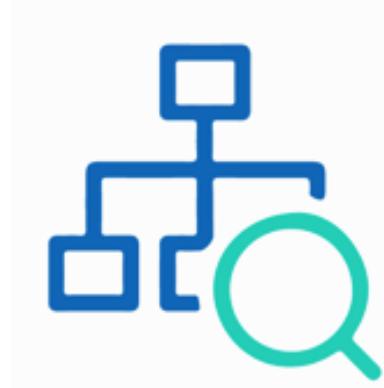


## Virtual Cloud Network に わたるセキュリティの有効化

NSX-T を含む NSX Data Center のためのマイクロセグメンテーション計画とネットワーク可視化

## SaaS サービスでの提供

米国だけでなく、他の国でも提供を検討中  
**多要素認証**でサービスアクセスへのセキュリティ強化



## マルチクラウドの可視化に最適

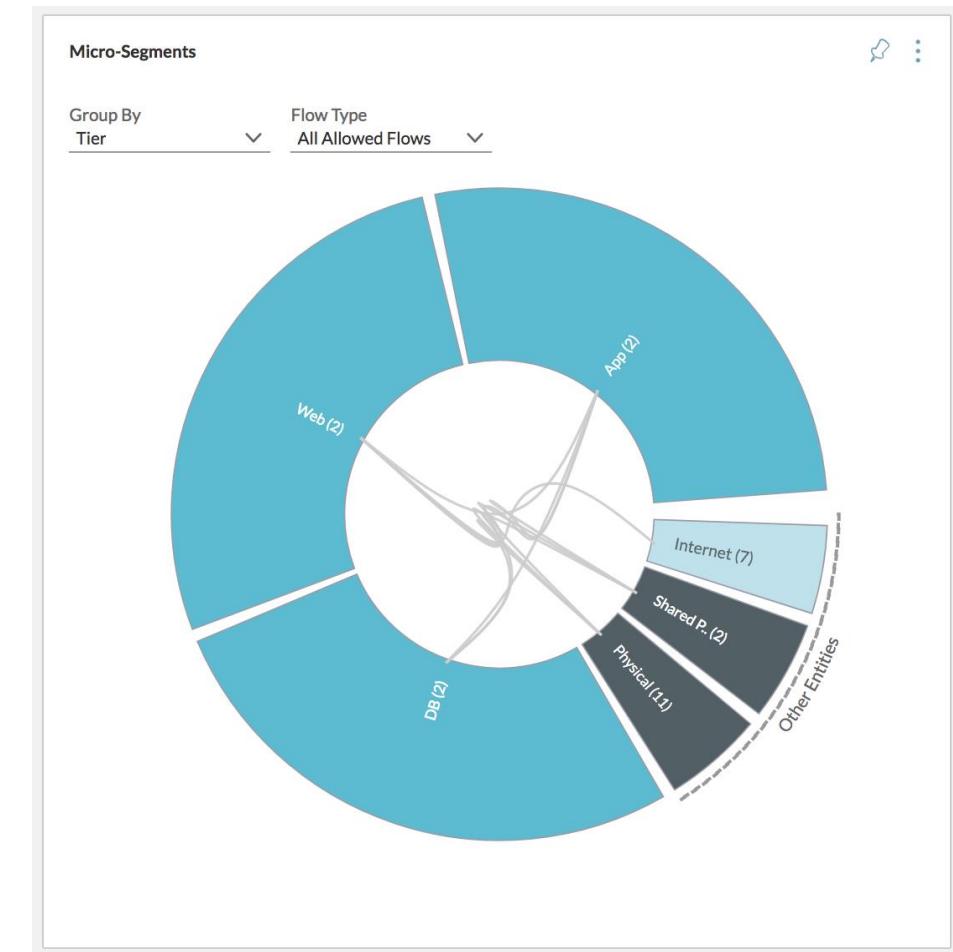
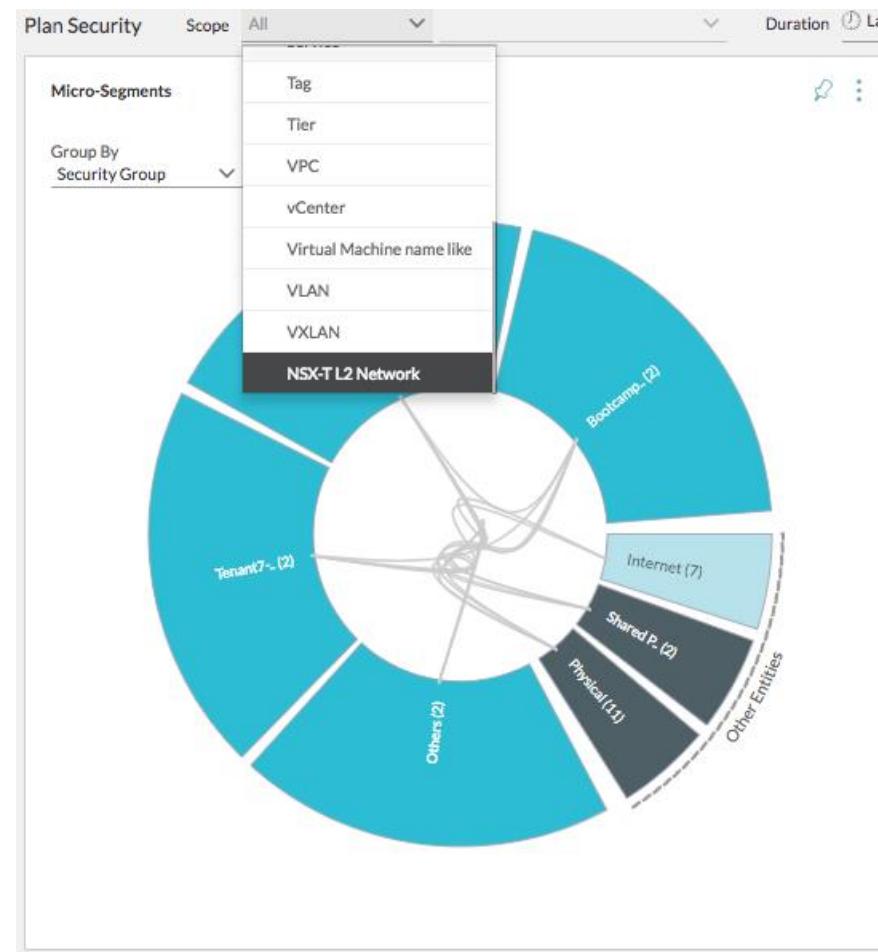
**カスタムなダッシュボード**, Cisco ASA ファイアウォールのサポートや サポート済みチェックポイントファイアウォールサポートの強化

# NSX-T フローとマイクロセグメンテーション

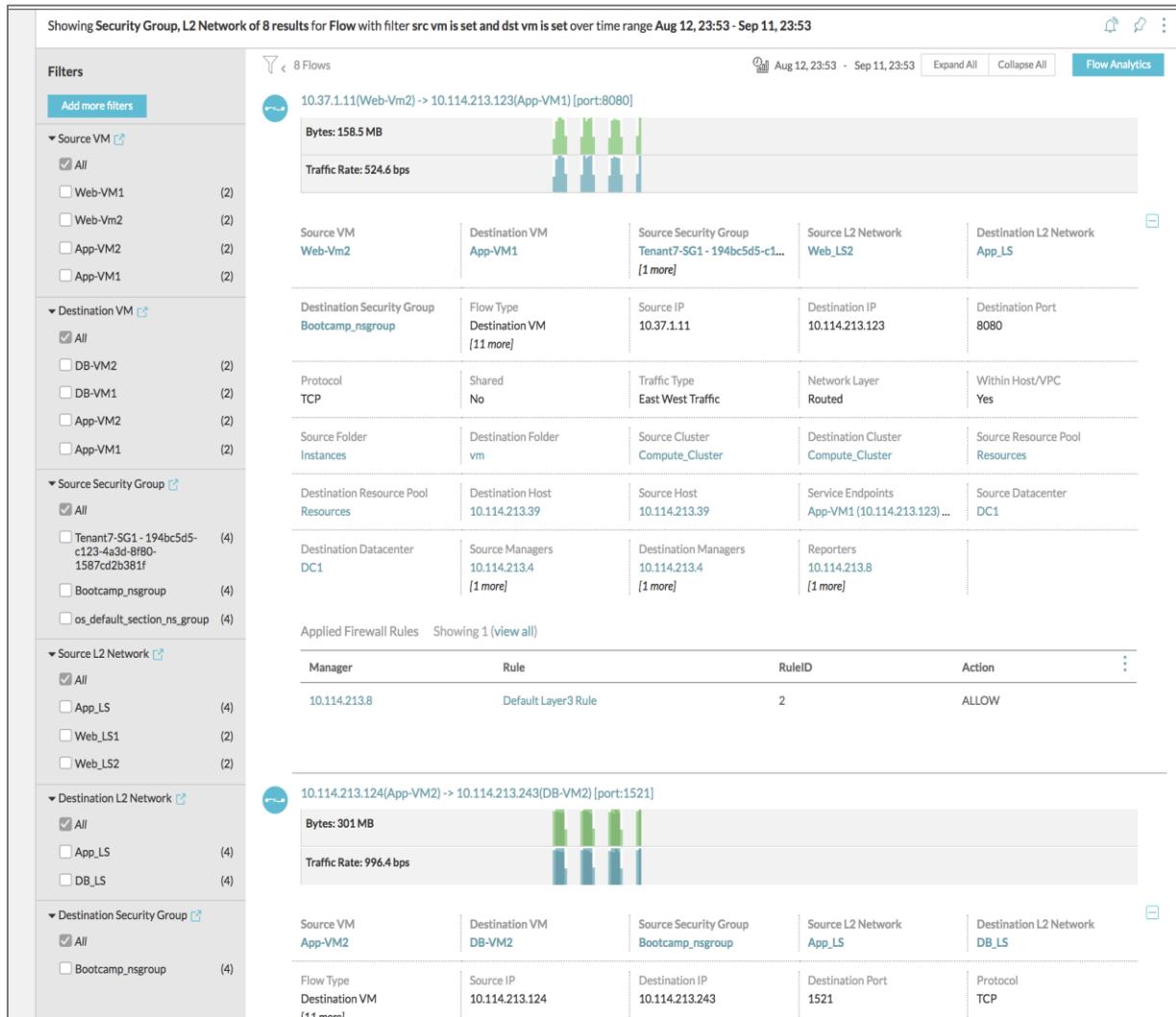
Plan Security と  
Micro-Segments で  
NSX-T 関連のエン  
ティティが利用可能

スコープで NSX-T  
エンティティの表示  
NSX-T L2 ネット  
ワーク  
タグ

推奨ファイアウオ  
ールルールに対して実  
際に適用されたファ  
イアウオールルール  
をマッチング



# NSX-T フロー 詳細

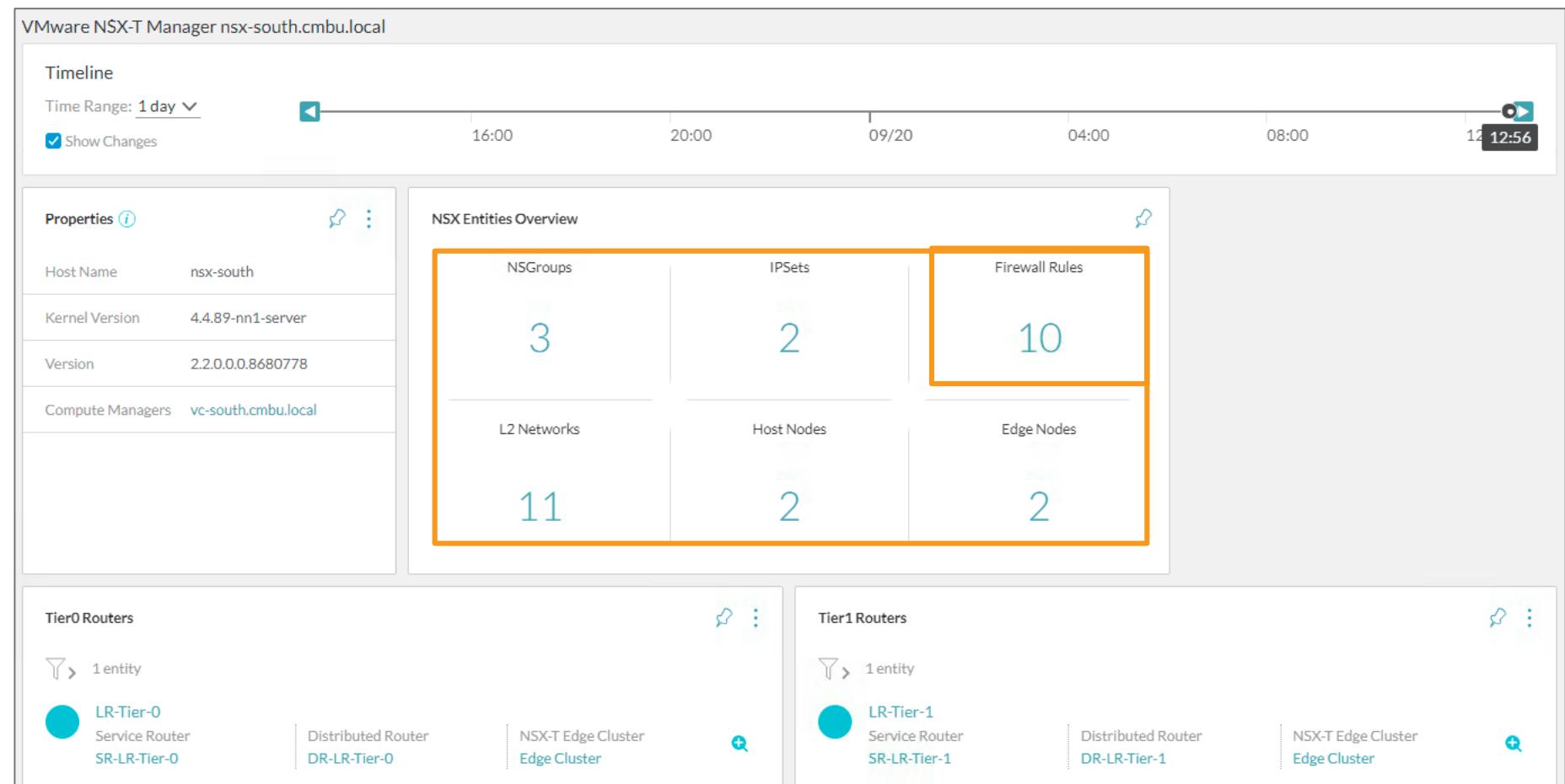


NSX-T 関連エンティティを含むためにフロード強化  
VIF  
論理スイッチ  
セキュリティ  
グループ  
トランスポート  
ノード

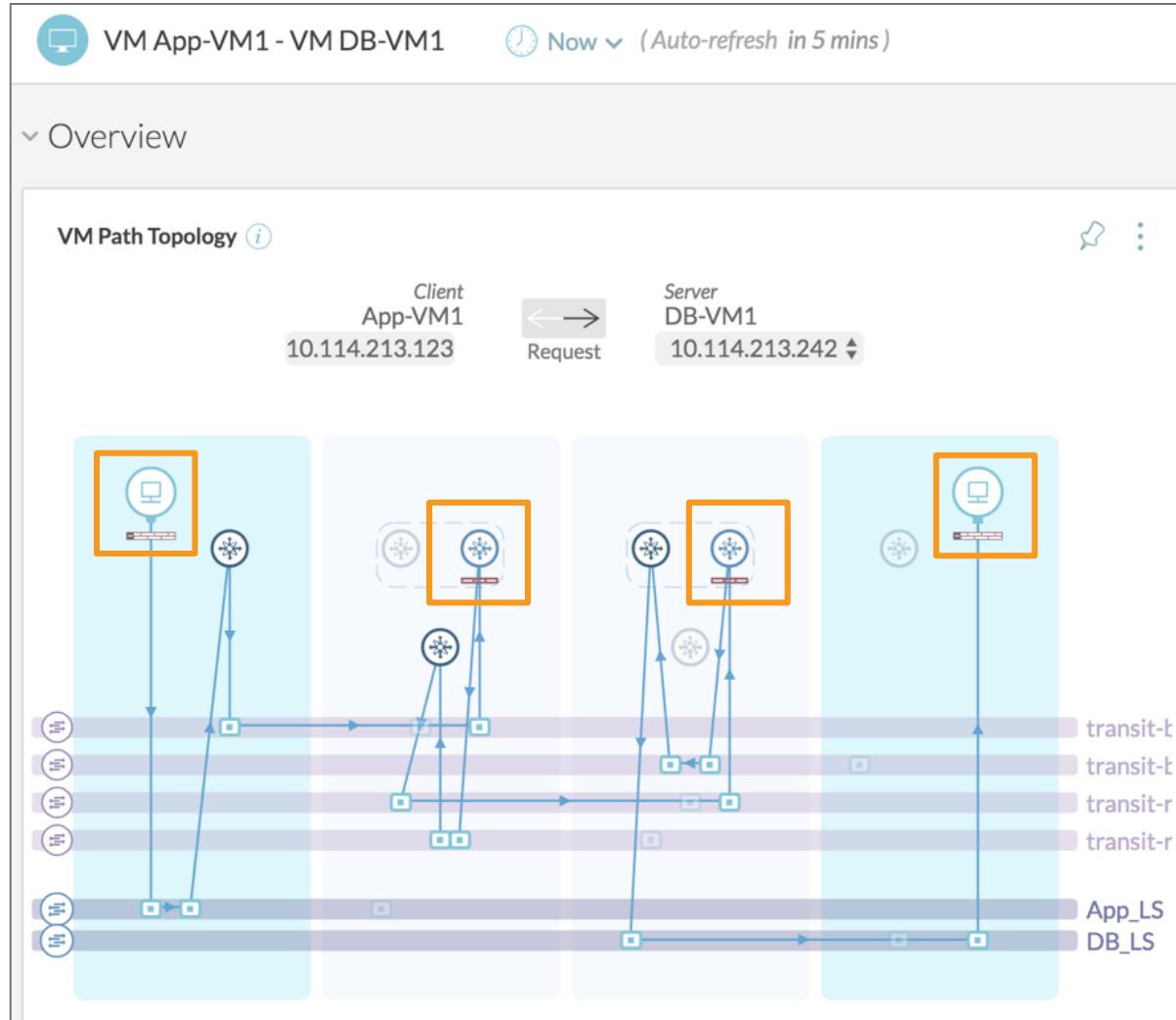
DFW によって適用されたファイアウォール ルール ID 確認

# NSX-T Manager ダッシュボード

ノード, L2 ネット  
ワーク, ファイア  
ウォールルール, 論理  
ルータの数の概要を  
提供



# NSX-T VM 間パス



NSX for vSphere 同様のパス表示

パス内の分散ファイアウォールと Edge ファイアウォール ルールを確認

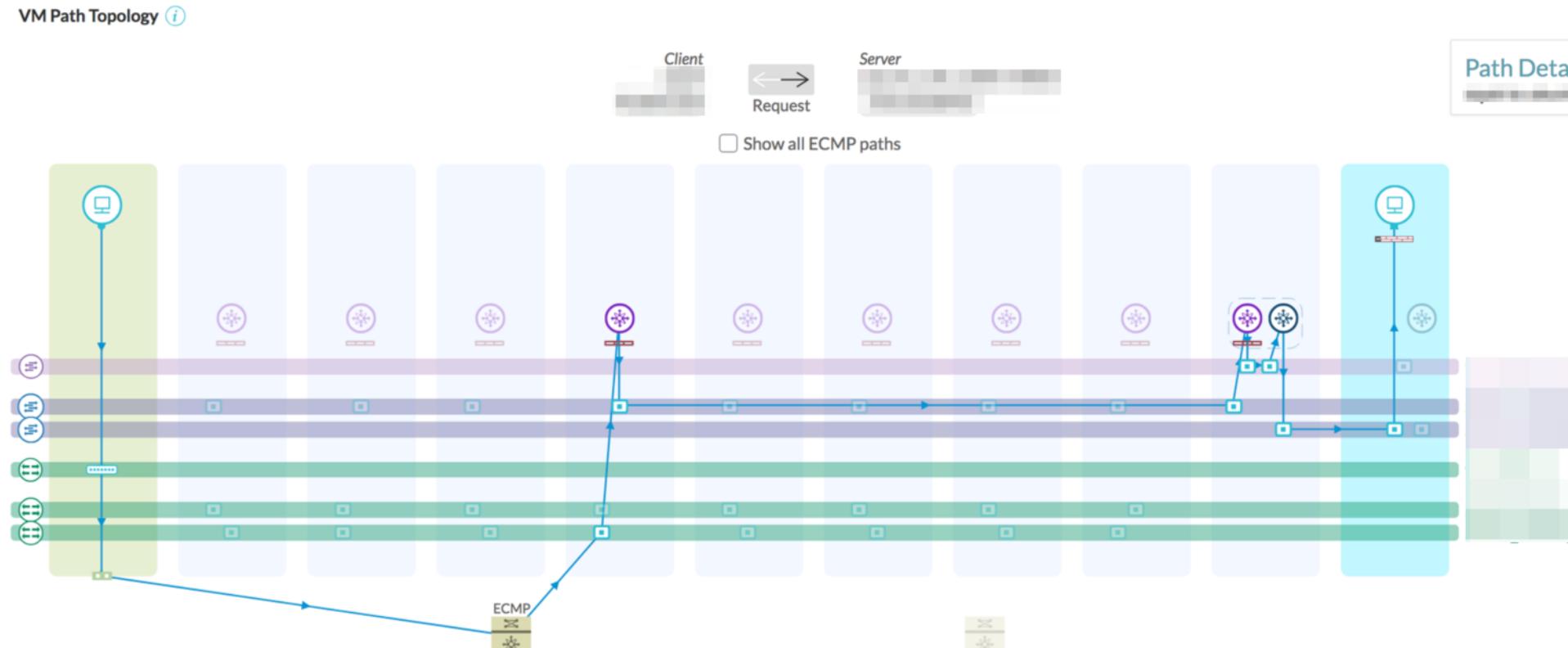
# NSX for vSphere の VM から NSX-T の VM へのパス

NSX Data Center 混在環境

NSX for vSphere と  
NSX-T 間のパス情報

物理と ECMP パスと  
ともに表示

NSX-T トランスポー  
トノード、ルータの  
Tier-0/1 ルータ、  
Edge の詳細



# SaaS サービスとしての Network Insight

The screenshot shows the VMware Cloud website with the Network Insight service page. The top navigation bar includes links for VMware Cloud, 製品とサービス, 目的で探す, パートナーを検索, イベント, コミュニティ, ログイン, and the VMware logo. Below the navigation is a secondary menu with tabs for 概要 (selected), 料金, FAQ, and リソース, along with a 無料で開始 button. The main content area features a dark background with white text and icons. It highlights "Network Insight" and its ability to optimize network security for private, public, and hybrid clouds. A large "FREE" button is visible. To the right, there's a section titled "Network Insight の導入" (Introduction) with sub-sections for "Network Insightによるアプリケーションの保護、移行、可用性確保" (Application protection, migration, and availability assurance) and two icons: one of a circuit board and another of a hand pointing at a screen.

VMware Cloud 製品とサービス 目的で探す パートナーを検索 イベント コミュニティ ログイン ホーム | 製品とサービス | Network Insight

概要 料金 FAQ リソース 無料で開始

Network Insight  
プライベート、パブリック、ハイブリッド、全てのクラウドのネットワークセキュリティを最適化

無料で開始

Network Insight の導入  
Network Insightによるアプリケーションの保護、移行、可用性確保

デモ：ハンズオン ラボ 無償でお試しください AdChoices

SaaS サービスとして提供 (US、イギリスのみ)

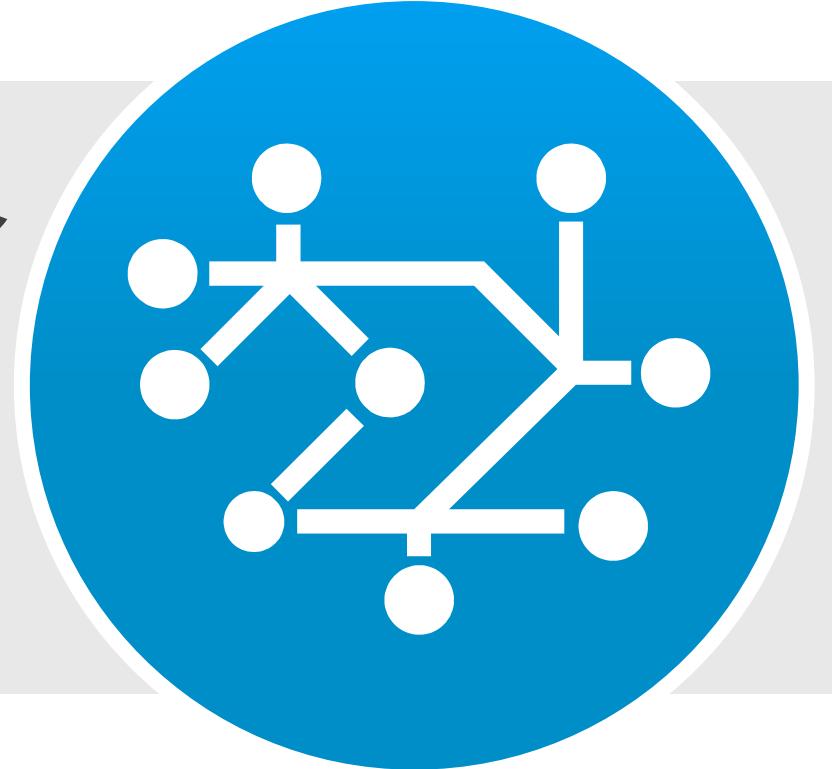
他の国や地域での提供を検討中（日本は未定）

無料でお試し提供中

<https://cloud.vmware.com/jp/network-insight>

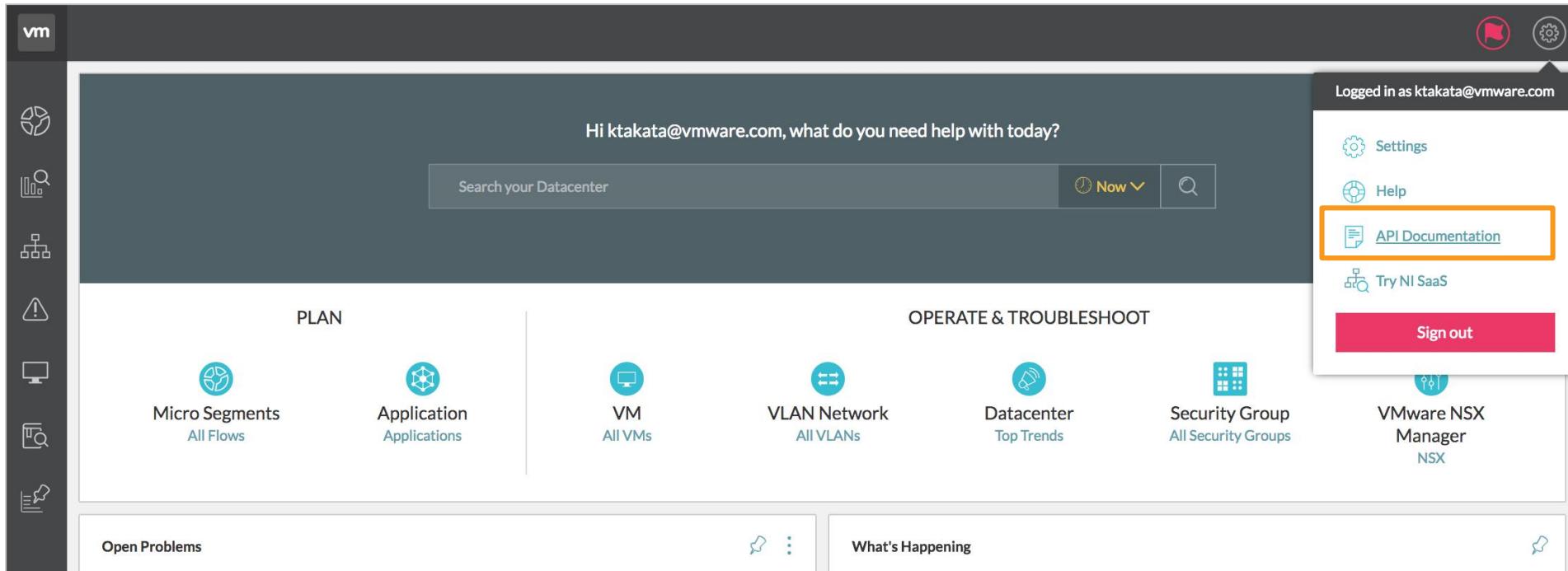
注：下記は米国にてサービス提供

ネットワークとセキュリティ  
をもっと改善 & 活用  
しましょう!



# 参考：役立つ参考情報

- API – vRNI の右上にある Profile で、API Documents があります



- PowervRNI の活用 – <https://www.vmguru.com/series/powervrni/>  
ユースケース例: データソース、アプリケーション グループの追加や設定



ありがとうございました。