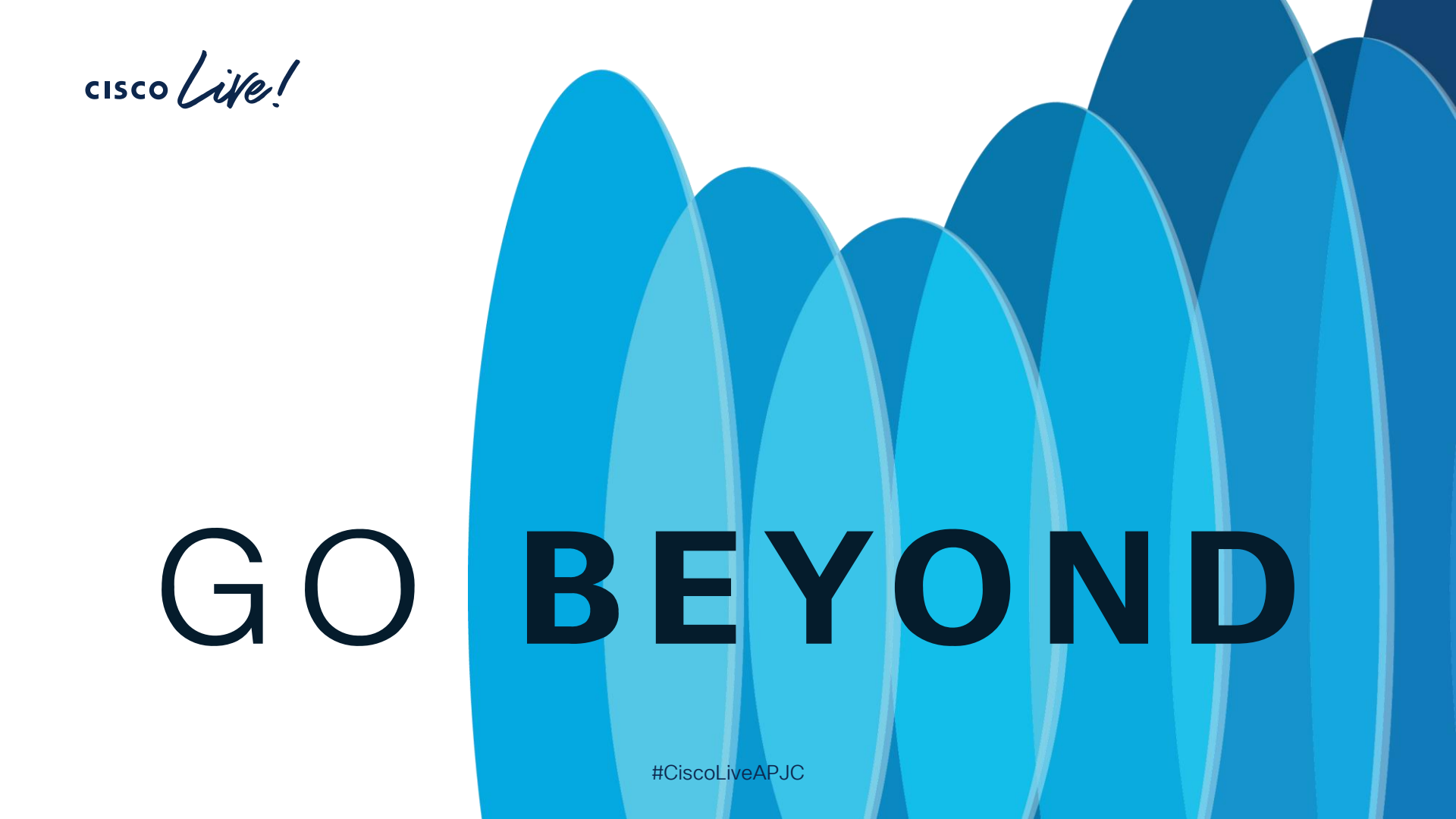

cisco Live!
GO BEYOND
#CiscoLiveAPJC

Enhancing Network Integrity with Catalyst SD-WAN

Deep Dive into End-to-End Security

Shamil Fernando - Global Solutions Architect

Session ID BRKENS-2567

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-2567

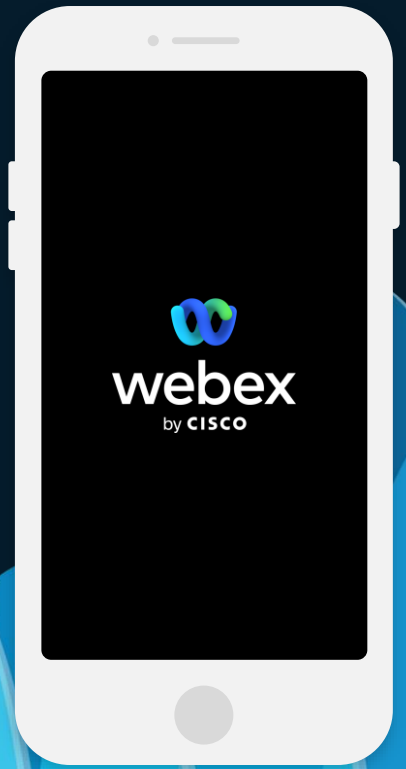
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



cisco Live!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Catalyst SD-WAN
- Architecture
- Fabric Security
- Next-Gen Firewall in SD-WAN
- Secure Access Service Edge (SASE)
- ISE Integration & Segmentation
- Management and Reporting
- Wrap-Up
- Q&A

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Today's application and security

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Catalyst SD-WAN Architecture

cisco Live!

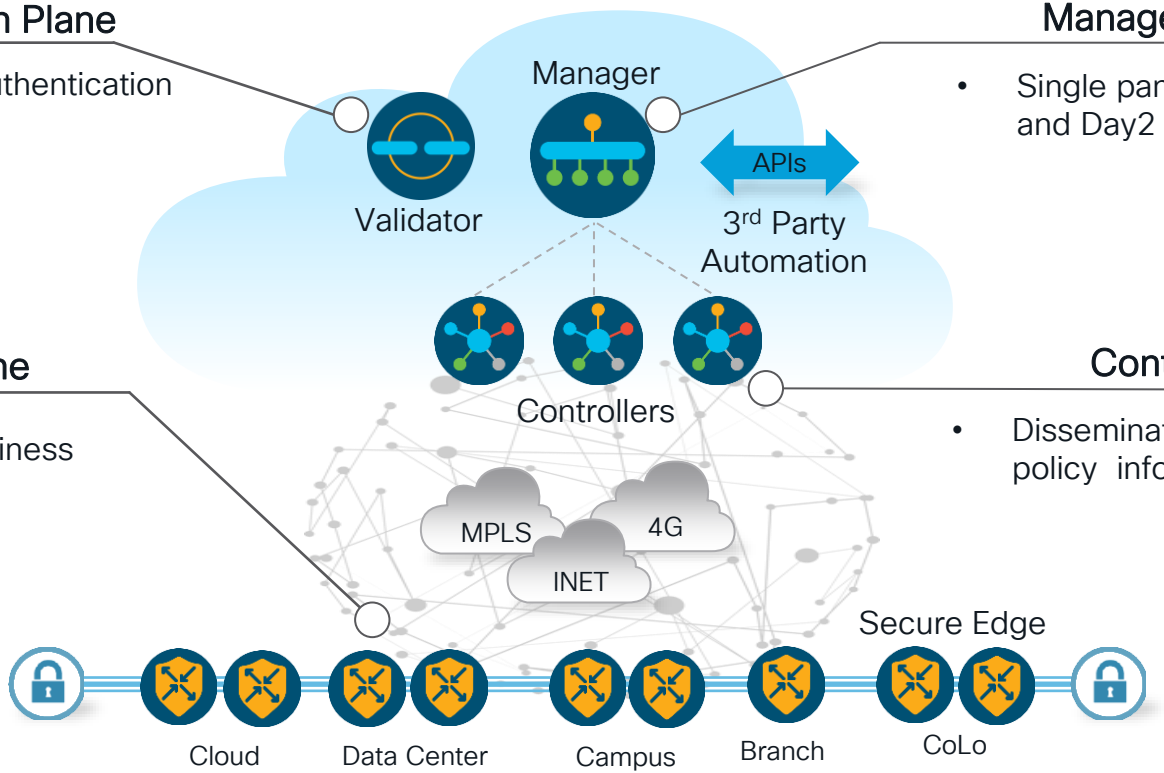
Catalyst SD-WAN Architecture

Orchestration Plane

- First point of authentication

Management Plane

- Single pane of glass for Day0, Day1 and Day2 operations



Data Plane

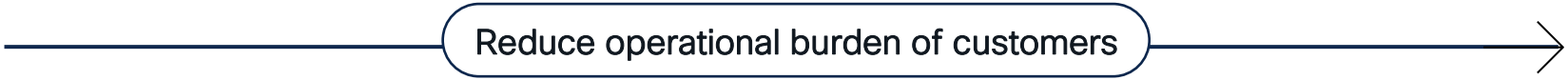
- Implements business intent policies

Control Plane

- Disseminates control plane and policy information between Edges

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric Deployment Models



Customer Hosted
(On-Prem, AWS & Azure)

- Customer Data Center
- MSP Data Center

Cisco Hosted
(AWS & Azure)

- Standard Environment (Shared and Dedicated)
- Certified Environment (PCI, SOC2, ISO, C5, etc.)
- Gov. Cloud (FedRAMP)

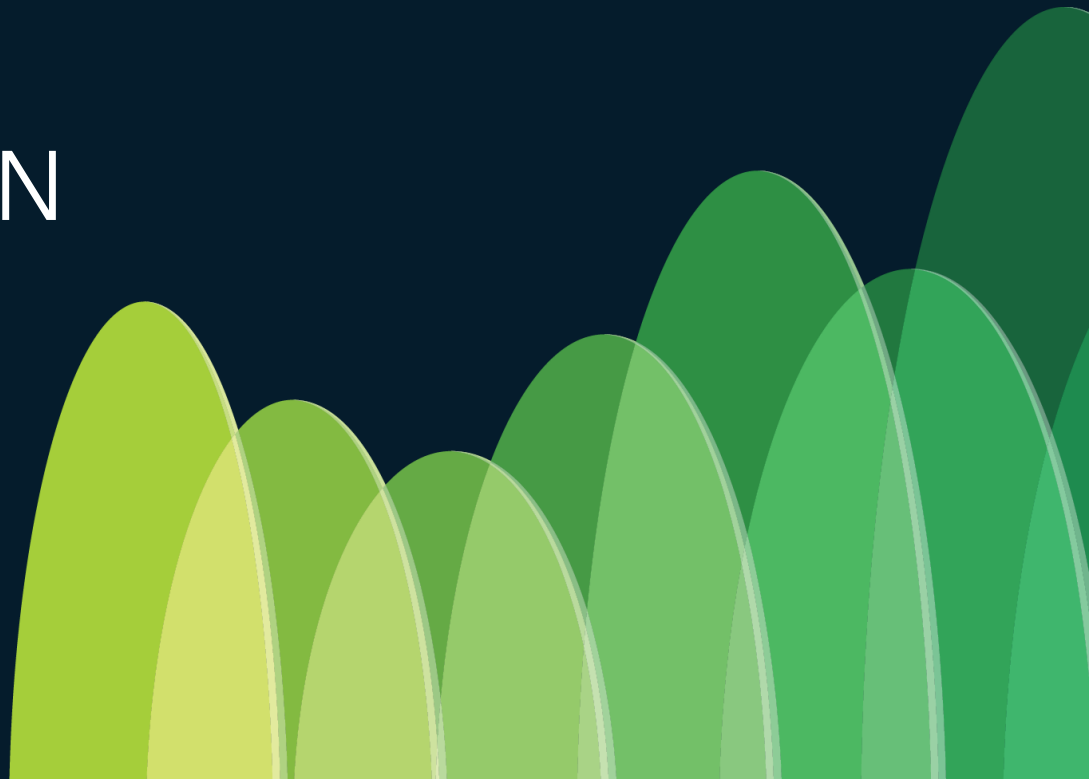
Cloud-delivered
(SaaS)

- Life Cycle Management of SD-WAN Fabric
- Agile and scalable service access
- Operational simplicity
- Rich analytics providing actionable insights

Flexible deployment models aligned to your business needs

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Catalyst SD-WAN Fabric Security



cisco Live!

Catalyst SD-WAN Fabric Security

NGFW in IOS-XE
Secure Branch to Branch, Branch to Internet

- Firewall
  Stateful & App-aware NGFW
  IPv6 support
- Segmentation
  Micro & Macro Segmentation
- Intrusion Prevention System
  (IPS) - Enhanced throughput with Snortv3
- TLS Decryption
  TLS encrypt/decrypt for security inspection
- Advanced Malware Protection
  File Reputation
- Sandboxing
  Secure Malware Analytics
- URL Filtering
- DNS Layer Security
- Live Signature
- Cisco ISE Integrations
- Unified Logging
- Dynamic Core Allocation

SD-WAN Integration with Cloud Security (SSE)

- Tunnel Automation
- Simplified Configuration
- Layer-7 Health Check
- Traffic Load Balancing
- Service Resiliency
- Multi-Tunnel support

Cisco SASE Integration
Secure Branch to Internet

- Cisco Umbrella
- Cisco Secure Access (NEW)
- Cisco+ Secure Connect

3rd Party Integration

- zscaler
- paloalto NETWORKS
- CLOUDFLARE
- Microsoft SSE
- netskope

Fabric Security
Confidentiality, Integrity, and Availability

- Encrypted
  Control Plane
- HW Based
  Device Authentication (SUDI)
- Encrypted
  Data Plane
- Enhanced Security
  Pairwise keys
- DDoS Protection

Certification & Compliance
Industry standards, fostering trust

- PCI-DSS
- SOC2/SOC3
- C5
- 27001, 27017 27018, 27701
- FedRAMP
- FIPS 140-2

Monitoring & Visibility

- SD-WAN Manager
  SecOps Dashboard
- Microsoft Sentinel
- splunk>

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

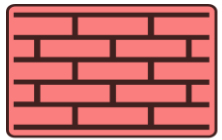
Secure Edge

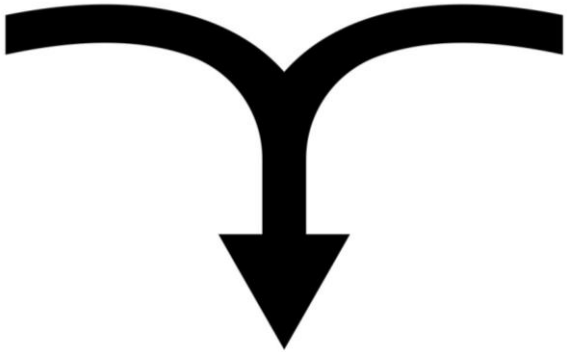
Network Team

Router (Private Links)

Security Team

Firewall (Public Links)





Cisco Catalyst Secure Edge

(Private & Public Links)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric Security

Secure Edge
Perimeter **Protection**

- Explicit Deny
- Zones Based Architecture
- No Open Ports
- DDOS Mitigation
- Trust Anchor Module (TAm)
- Secure Boot of Signed Images
- Runtime Defenses (RTD)

Onboarding & Authentication

- Devices Onboarding Process
- Zero Trust
- Certificate-based Authentication & Whitelisting
- Automate Custom Certificate Authority (CA)
- Management through using SD-WAN Manager

Transport Security

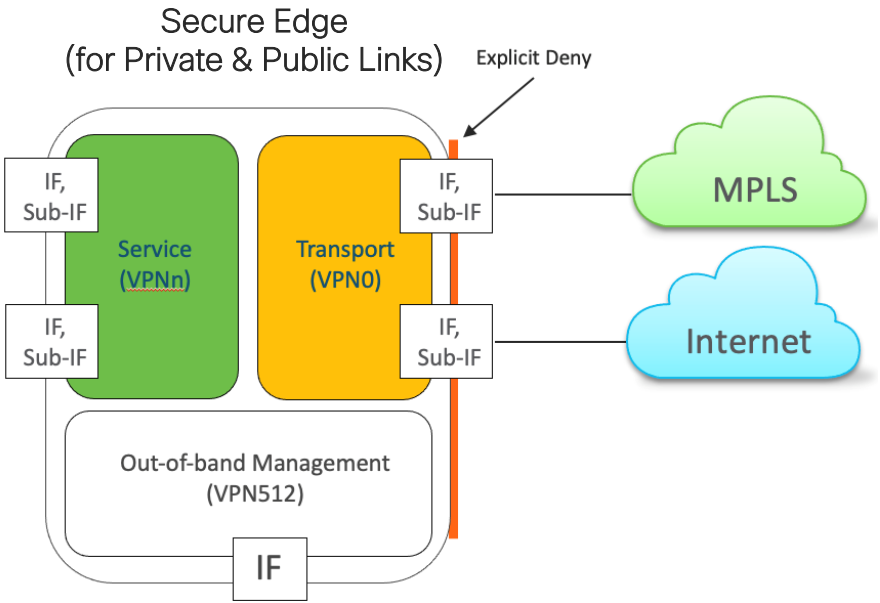
- IKE less IPsec (Key exchange using a controller, high scale)
- Key - Using RNG (NIST SP 800-90A)
- Key Rotation - 24hr Default
- Anti-Replay Protection

Least Access Principle

- Segmentation (VRF) - True VRF with separate route table & different topology each VRF
- Overlay Management Protocol (OMP)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Perimeter protection



- Explicit Deny
- Zones Based Architecture
- No Open Ports
- DDOS Mitigation
- VPNs are isolated from each other, each VPN has its own forwarding table
- Reachability within VPN is automatically advertised by the OMP

Trust Zone
Untrust Zone

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco trustworthy technologies

Secure Boot of Signed Images

- Prevents malicious code from booting on a Cisco platform
- Automated integrity checks
- Monitors startup process and shuts down if compromised
- Faster identification of threats

Trust Anchor module (TAm)

- Tamper-resistant chip with X.509 cert installed at manufacturing
- Provides unique device identity and anti-counterfeit protections
- Secure, non-volatile on-board storage and RNG/crypto services
- Enables zero-touch provisioning and minimizes deployment costs

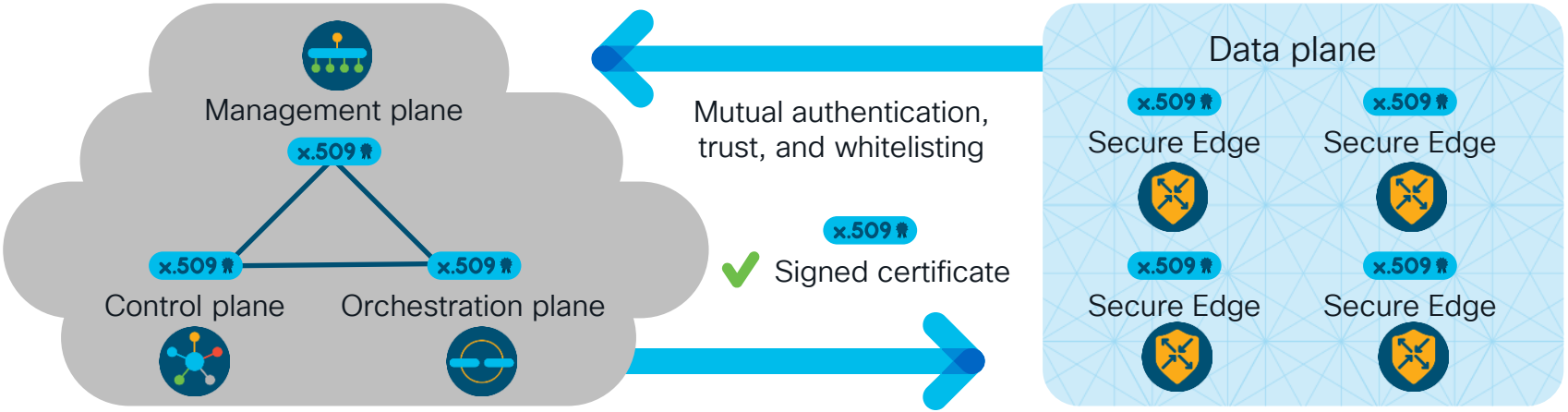
Runtime Defenses (RTD)

- Protects against injection of malicious code into running software
- Makes it harder for attackers to exploit vulnerabilities in running software
- Runtime technologies include ASLR, BOSC, and X-Space

Trustworthy technologies enhance the security and resilience of Cisco solutions

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fabric with Zero-Trust authentication



- Mutual certificate-based authentication
- Validator validates Controller and Manage certificate serial numbers against authorized white-list

- Embedded device identity (TPM)
- AES 256-GCM-based encryption
- Frequent key rotation (default: 12 hours)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure bring-up with approval

Chassis Number	Certificate Serial	Hostname	IP Address	Validate ↓
9391da23-f0d1-4259..	0334D73E5EC036F87ABE...	DataCenter	1.1.1.5	invalid | staging | valid
4de0b85f-a2ae-42ec...	585A0084DEA8396DD77B..	RemoteSite	1.1.1.4	invalid | staging | valid
5f05358a-bef7-4e15...	248792F938E6EA8BEE6FD..	AWS	1.1.1.6	invalid | staging | valid

- Single stage (Zero Touch Provisioning) – Identity is automatically trusted
- Two stage (One Touch Provisioning) – Identity is not automatically trusted. Requires administrator validation.
- Staging Mode – Identity is automatically trusted for control, but not for data. Requires administrator validation.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Next-Gen Firewall in SD-WAN

cisco Live!

NGFW in SD-WAN

NGFW in SD-WAN
Secure Branch to Branch, Branch to Internet

- **Firewall**
  Stateful & App-aware NGFW
  IPv6 support
- **Segmentation**
  Micro & Macro Segmentation
- **Intrusion Prevention System**
  (IPS) - Enhanced throughput with Snortv3
- **TLS Decryption**
  TLS encrypt/decrypt for security inspection
- **Advanced Malware Protection**
  File Reputation
- **Sandboxing**
  Secure Malware Analytics
- **URL Filtering**
- **DNS Layer Security**
- **Live Signature**
- **Cisco ISE Integrations**
- **Unified Logging**
- **Dynamic Core Allocation**

SD-WAN Integration with Cloud Security (SSE)

- Tunnel Automation
- Simplified Configuration
- Layer-7 Health Check
- Traffic Load Balancing
- Service Resiliency
- Multi-Tunnel support

Cisco SASE Integration
Secure Branch to Internet

- Cisco Umbrella
- Cisco Secure Access (NEW)
- Cisco+ Secure Connect

3rd Party Integration

- zscaler
- paloalto NETWORKS
- CLOUDFLARE
- Microsoft SSE
- netskope

Fabric Security
Confidentiality, Integrity, and Availability

- **Encrypted**
  Control Plane
- **HW Based**
  Device Authentication (SUDI)
- **Encrypted**
  Data Plane
- **Enhanced Security**
  Pairwise keys
- **DDoS Protection**

Certification & Compliance
Industry standards, fostering trust

- PCI-DSS
- SOC2/SOC3
- C5
- 27001, 27017 27018, 27701
- FedRAMP
- FIPS 140-2

Monitoring & Visibility

- **SD-WAN Manager**
  SecOps Dashboard
- Microsoft Sentinel
- splunk>

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Next-Gen Firewall in Catalyst / Meraki

Meraki MX

Simplified Operations — Industry pioneers in cloud management and simplicity with hitless updates to threat detection engine, as-a-service

Catalyst WAN

Extensive Capabilities — Our Combined industry leading and most extensive routing capabilities powered by Cisco security ecosystem

Talos Threat Intelligence

Snort3 IPS

Secure Client

Secure Connect (SASE)

eXtended Detection and Response

ThousandEyes

Identity Services Engine

Duo Posture and Multifactor Authentication

NBAR & SD-AVC

Secure Access (SSE)

Malware Analytics

Splunk

Full stack network, observability, security and AI

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Superior Security, Independently Verified

BETTER TESTING

Uniquely designed to match **real-world conditions** instead of a lab environment

98% EFFECTIVE

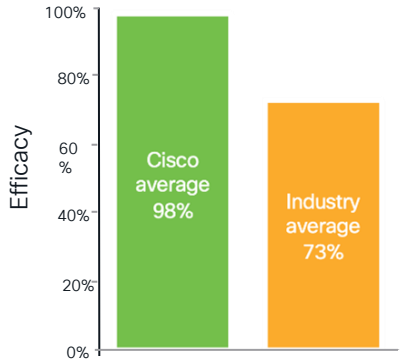
Cisco malware efficacy across 11 real-world exploit categories

25% BETTER

Cisco malware efficacy compared to the industry average

Miercom

Independent malware efficacy testing



Exploits tested

- Active threat
- Advanced evasive threat
- Advanced persistent threat
- Backdoor exploit
- Bot network exploit
- Legacy malware
- Modified malware
- Malicious docs
- Polymorphous zero +1 day
- Remote access trojan
- Tor trojan exploit

- **External link** https://miercom.com/cisco/

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security efficacy & performance

Up to 186%

Increase in throughput on average

98%

Next-Generation Firewall (NGFW) Security Efficacy

100%

Efficacy for URL-Filtering*

EMIX Traffic Profile (DIA+ZBFW+IPS+URLF+AMP)

Enhanced Security Throughput

	Release 20.9		Release 20.12.3		
Large Branch	1750 Mbps	165%	4640 Mbps	7%	4950 Mbps
Large Branch	1470 Mbps	48%	2178 Mbps	33%	2900 Mbps
Medium Branch	328 Mbps	130%	757 Mbps	30%	980 Mbps
Small Branch	75 Mbps	240 %	260 Mbps	11%	290 Mbps

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

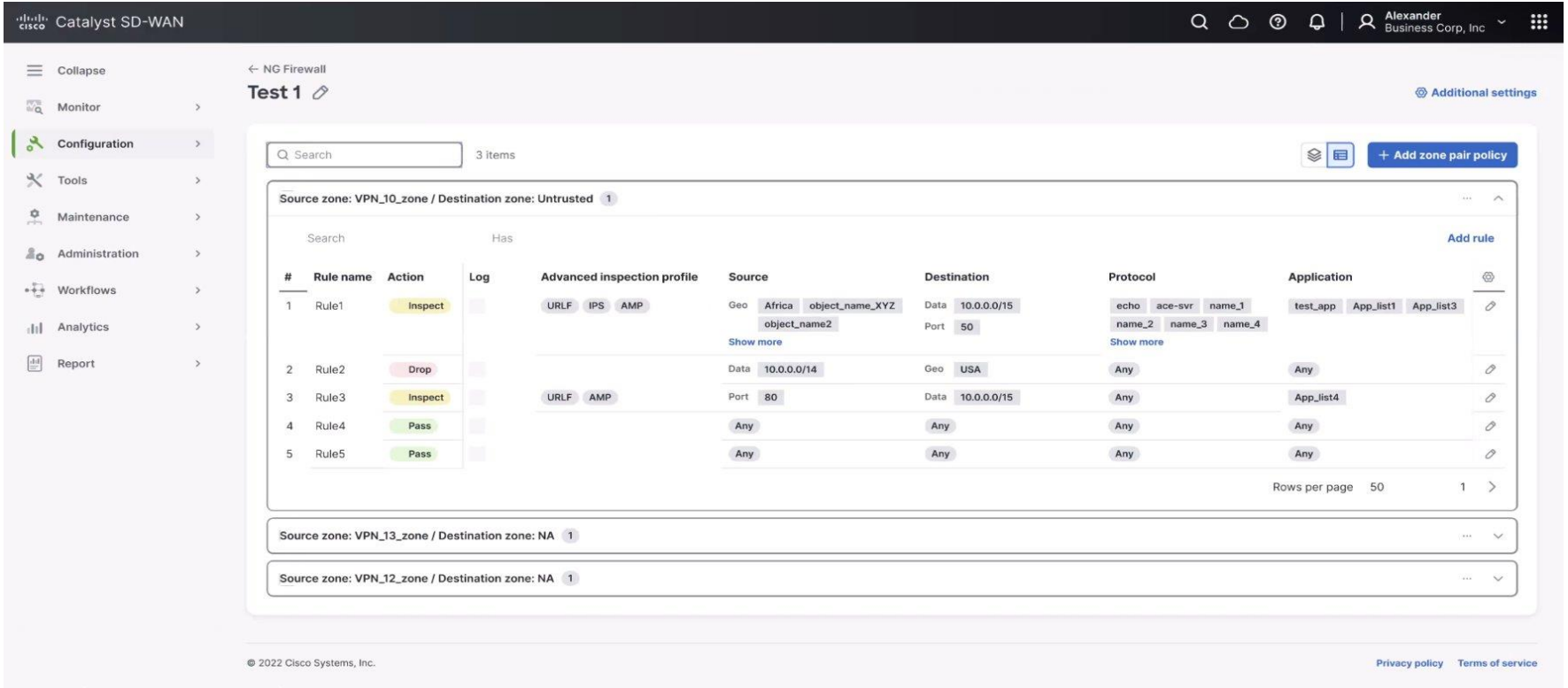
Catalyst SD-WAN- NGFW

Area	Functionality	Cisco (FTD)	SD-WAN Security Engine (Current)	SD-WAN Security Engine (New)
Firewalling	L3-L4 Firewalling	Yes	Yes	Yes
	Identity Firewalling (User/Groups)	Yes	No	Yes
	Dynamic Attributes	Yes	No	Yes
	Time based AC rules	Yes	No	Yes
	Geolocation	Yes	Yes	Yes
	FQDN & Wildcard FQDN	Yes	Yes	Yes
	Destination List (IP, URL, Port)	Yes	No	Yes
Threat Protection	Security Intelligence (IP & URL)	Yes	No	Yes
	AppID	Yes	Yes	Yes
	Content Filtering (Cat & Rep)	Yes	Yes	Yes
	Deep Packet Inspection (IPS)	Yes	Yes	Yes
	Protocol Inspection (Network Analysis Policy)	Yes	No	Yes
	Malware Protection (AMP)	Yes	Yes	Yes
	Malware Dynamic Analysis (TG)	Yes	Yes	Yes
Encrypted Traffic	Decryption Policy	Yes	Yes	No
	Encrypted Visibility Engine	Yes	No	No
Networking	Static and Dynamic Routing	Yes	NA	No
	NAT	Yes	NA	No
	QoS	Yes	NA	No
VPN	Site-to-Site VPN	Yes	NA	No
	RA-VPN	Yes	NA	No

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Improved SecOps experience

Firewall Rule table Expert view



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Cloud Security Control

- **Centralized Management:** Manage security policies and configurations across multiple Cisco devices from a single interface.
- **Policy Consistency**: Ensure consistent security policies across on-premises, cloud, and hybrid environments.
- **Automation and Orchestration**: Automate tasks and orchestrate workflows to improve efficiency and reduce errors.
- **Visibility and Reporting**: Gain comprehensive visibility and detailed reporting for compliance and auditing.
- **Simplified Operations**: Streamline operations with intuitive dashboards, policy templates, and guided workflows.
- **Integration**: Integrate with Cisco and third-party tools to enhance security posture and efficiency.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Access Service Edge (SASE)

cisco Live!

Secure Access Service Edge (SASE)

NGFW in IOS-XE
Secure Branch to Branch, Branch to Internet

- Firewall
  Stateful & App-aware NGFW
  IPv6 support
- Segmentation
  Micro & Macro Segmentation
- Intrusion Prevention System
  (IPS) - Enhanced throughput with Snortv3
- TLS Decryption
  TLS encrypt/decrypt for security inspection
- Advanced Malware Protection
  File Reputation
- Sandboxing
  Secure Malware Analytics
- URL Filtering
- DNS Layer Security
- Live Signature
- Cisco ISE Integrations
- Unified Logging
- Dynamic Core Allocation

SD-WAN Integration with Cloud Security (SSE)

- Tunnel Automation
- Simplified Configuration
- Layer-7 Health Check
- Traffic Load Balancing
- Service Resiliency
- Multi-Tunnel support

Cisco SASE Integration
Secure Branch to Internet

- Cisco Umbrella
- Cisco Secure Access (NEW)
- Cisco+ Secure Connect

3rd Party Integration

- zscaler
- paloalto NETWORKS
- CLOUDFLARE
- Microsoft SSE
- netskope

Fabric Security
Confidentiality, Integrity, and Availability

- Encrypted
  Control Plane
- HW Based
  Device Authentication (SUDI)
- Encrypted
  Data Plane
- Enhanced Security
  Pairwise keys
- DDoS Protection

Certification & Compliance
Industry standards, fostering trust

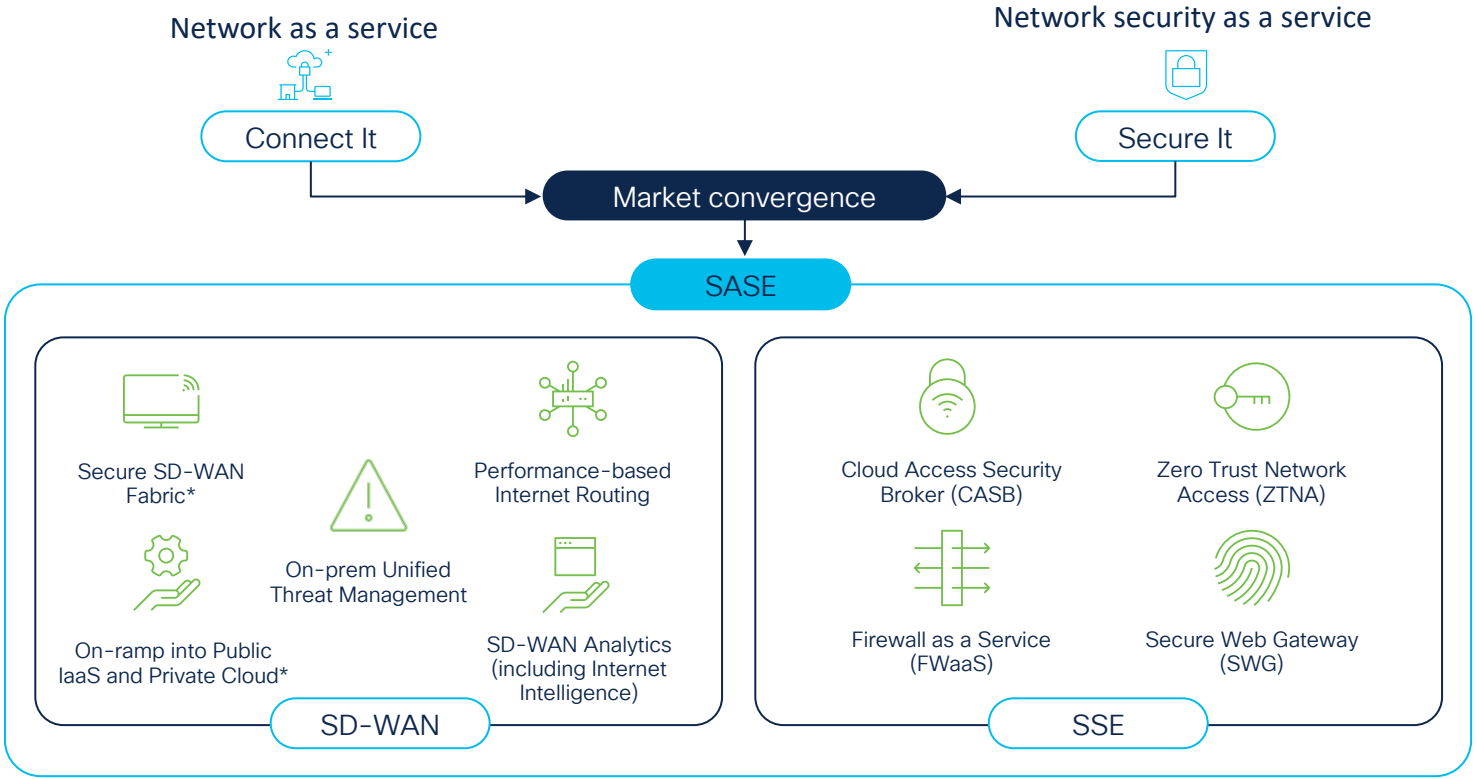
- PCI-DSS
- SOC2/SOC3
- C5
- 27001, 27017 27018, 27701
- FedRAMP
- FIPS 140-2

Monitoring & Visibility

- SD-WAN Manager
  SecOps Dashboard
- Microsoft Sentinel
- splunk>

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SASE: Unifying networking & security services



Catalyst SD-WAN

+

zscaler paloalto NETWORKS

netskope CLOUDFLARE

Microsoft SSE

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

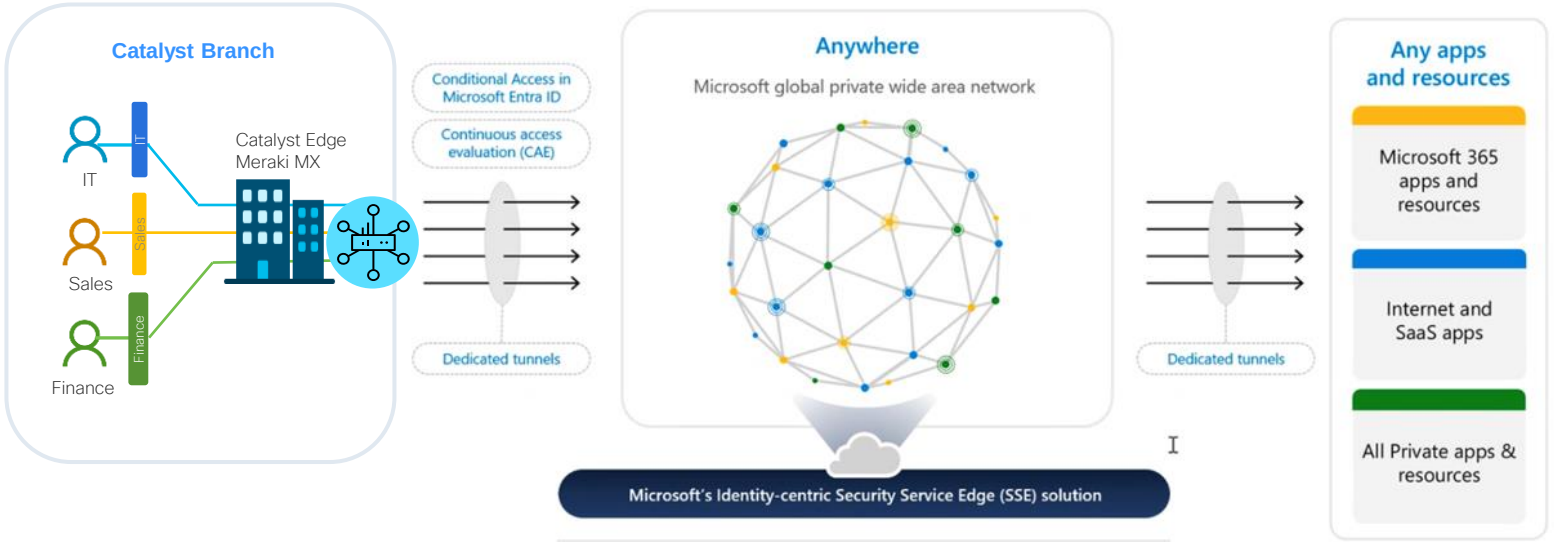
Catalyst SD-WAN & Cisco Secure Access

Seamless Secure Connectivity from Anywhere to Anything

	Available Today 2H CY2023	Summer 2H CY2024	**Late Fall** **2H CY2024**
Use Case	Secure Direct Internet Access from Branches	Integrated Admin Experience Context Sharing for Segmentation	Secure Private Application Access Distributed Policy Enforcement
Key Capabilities	• Automation between Catalyst and SD-WAN • Resilient connectivity to SSE • Higher Bandwidth Connectivity (8 Gig)	• Seamless Network Context Sharing for Internet bound traffic (VPN and SGT)	• Seamless Private access connectivity • Seamless Context Sharing for DIA & Private Access (VPN and SGT) • Leverage Catalyst for policy Enforcement • Cross launch Catalyst Management portal from Secure Access dashboard and vice versa

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Catalyst SD-WAN & Microsoft Entra



	Phase-1 (Branch Users)	Phase-2 (Identity based Security Policy) – TBD
Use Case	Secure Direct Internet Access (DIA) from Branches	Identity based Security policy
Key Capabilities	Manual Integration (June 2024) followed with Automated tunnels (Dec 2024) Simplified buying experience for customers - Cisco SD-WAN SKU on Microsoft Azure Marketplace – TBD	Context Sharing?

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Integration & Segmentation

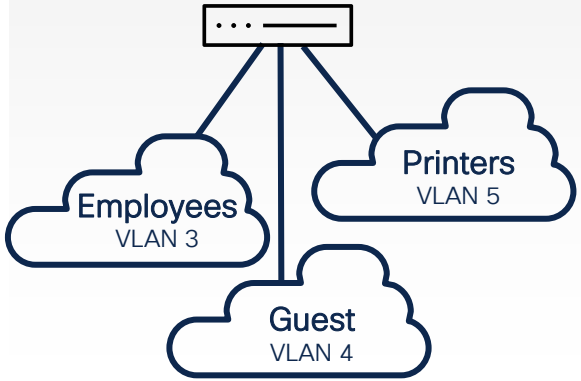
cisco Live!

Authorization enforcement options

Beyond RADIUS Access-Accept / Access-Reject

VLANs

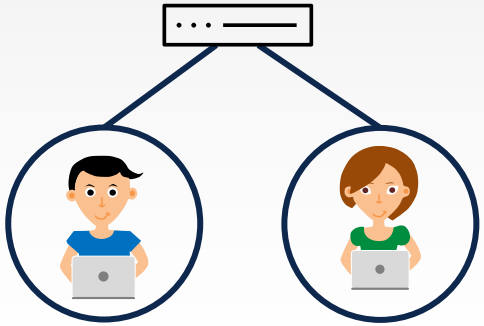
Dynamic VLAN Assignments



Per port / Per Domain / Per MAC

ACLs: DL, Named, DNS

Downloadable ACL (Wired) or
Named ACL (Wired + Wireless)



Employee

```
permit ip any any
```

Contractor

```
deny ip host <critical>
permit ip any any
```

Security Group Tags

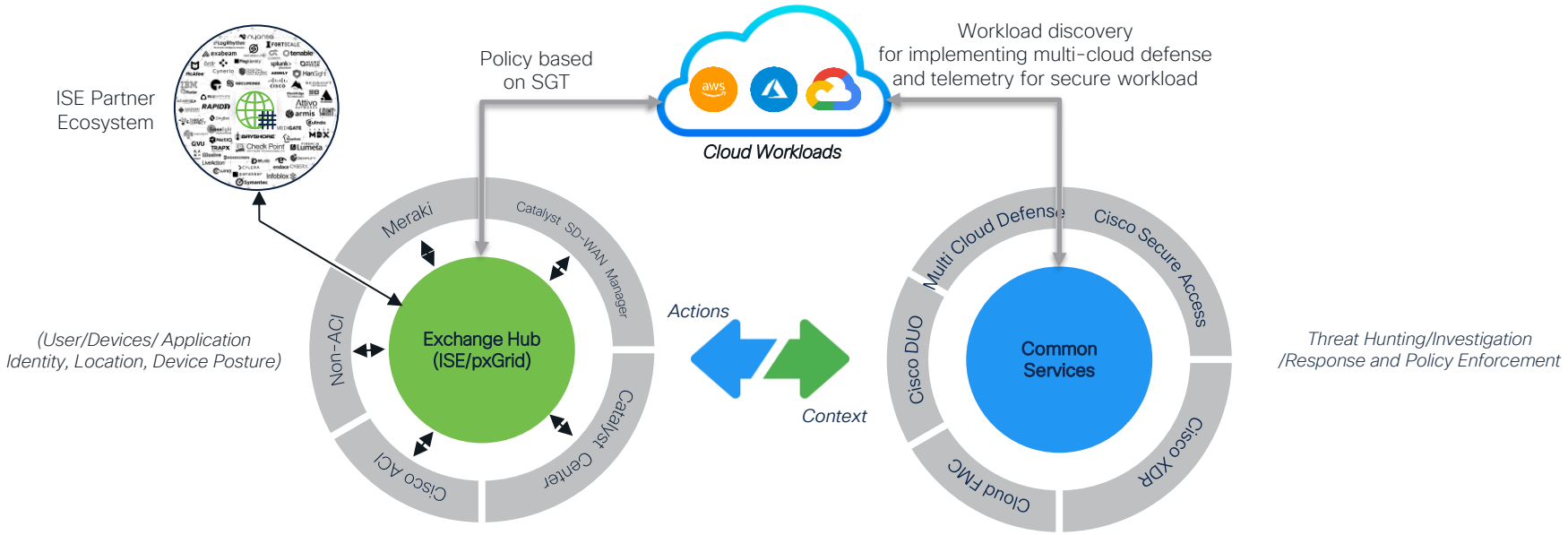
Cisco Group-Based Policy

16-bit SGT assignment and
SGT based Access Control

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Common policy for Cisco Networking Cloud

Normalizing and sharing context across domains



- Modular approach to support on-prem and cloud use cases
- Enables consistent zero-trust policies for multi-domain environments (Campus, WAN, Data Center, Cloud)
- Simplifies configuration by moving away from cloud- and vendor-specific tags to a single Cisco-defined Security Group Tag (SGT)
- Differentiated experience with ability to scale, support full range of use cases

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco journey in Zero Trust with ISE integration

Why Zero Trust :

- ✓ Digital Landscape Expanding
- ✓ Hybrid workforce
- ✓ Need tighter network security control

Zero Trust Principles:

- ✓ Never assume trust
- ✓ Always verify
- ✓ Enforce least privilege

Source	Destination	Application	Action
IP-Subnet	Any	Any	Inspect
192.168.1.0/24	SGT-Printer	Print	Allow
User-Joe	HR-Server	HTTPS	Inspect
User-Group Cisco.com/Contractor	Geo-EU	Video-Streaming	Drop
SGT-Users-Partner	www.in.cisco.com	HTTPS	Inspect

1 Identify the User/Device

- Cisco ISE is the **Identity Provider**
- ISE updates SD-WAN Manager

3a Continuously Check Posture

- ISE evaluates device **Security Posture**
- ISE updates **SGT** of device

2 Enforce Security Policy

- SD-WAN Manager is the **Policy Engine**
- Policy created based on **Identity**

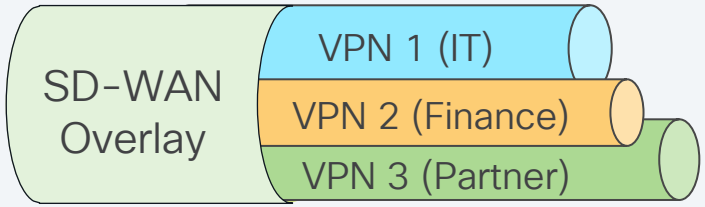
3b Respond to Change in Posture

- SD-WAN Manager learns of **change in security**
- Security policy is automatically updated

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Segmentation is built into SD-WAN

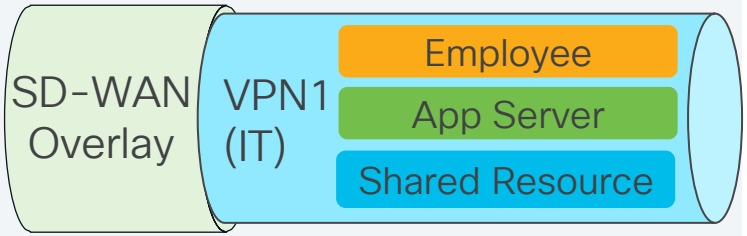
Macro Segmentation



VPN Level Segmentation

- IT VPN
- Finance VPN
- Partner VPN

Micro Segmentation

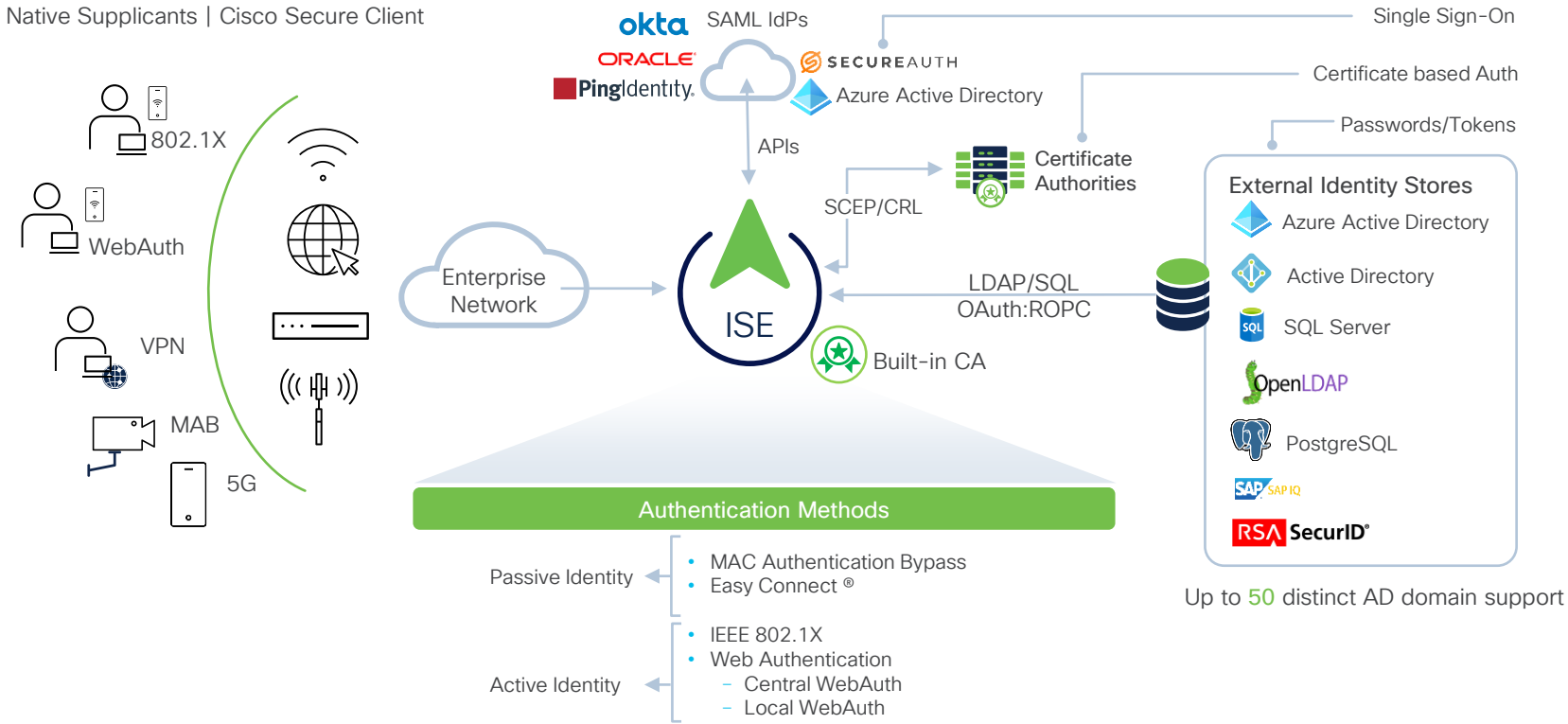


Group Level Segmentation
Example: IT VPN

- Employee
- App Server
- Shared Resource

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

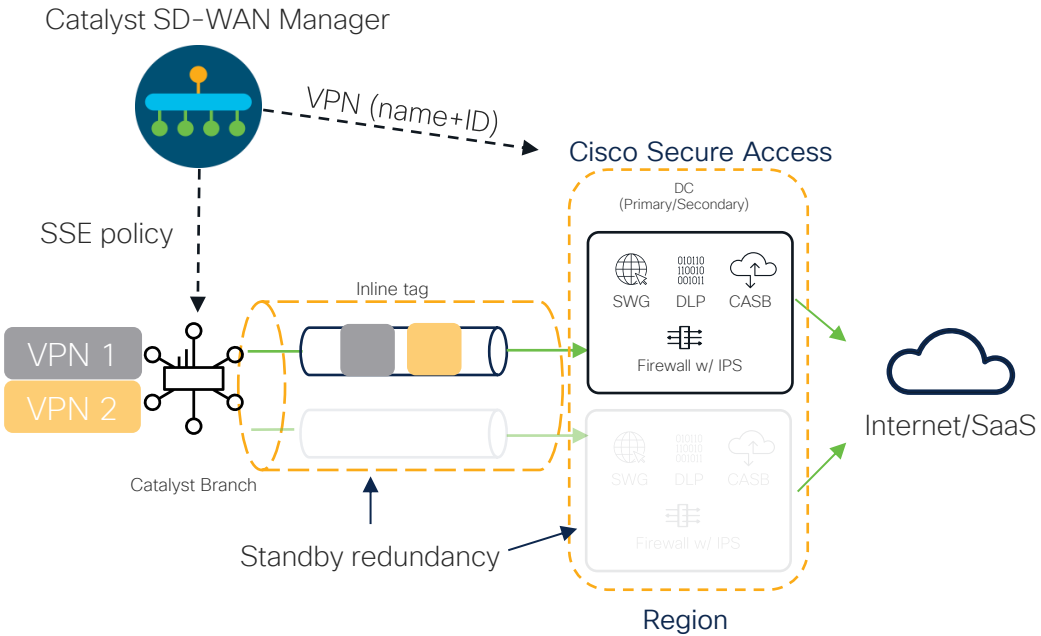
ISE Secure access control options



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Context-Sharing: Extending VPN-id segmentation to Cisco Secure Access

Catalyst SD-WAN + Cisco Secure Access

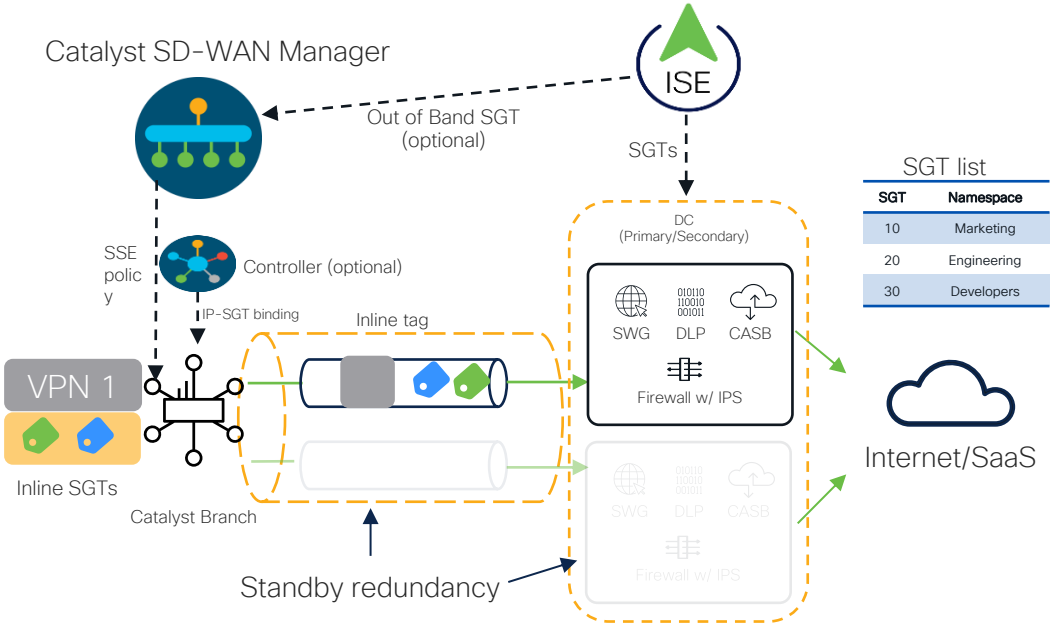


1. Catalyst Manager integrates with Cisco Secure Access using SSE cloud credentials.
2. Cisco Secure Access learns VPN identities using APIs (OOB)
3. In Catalyst SD-WAN Manager the Secure Service Edge policy group is configured to share VPN context in tunnels
4. Once tunnels are up, VPN identity is shared in the IPsec metadata header inline
5. VPN identities are leveraged in Secure Access internet access policies
6. Packets with VPN ID context are then subject to Secure Access policy match as source objects

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Context-Sharing: micro-segmentation (SGT) to Secure Access

Catalyst SD-WAN + Cisco Secure Access

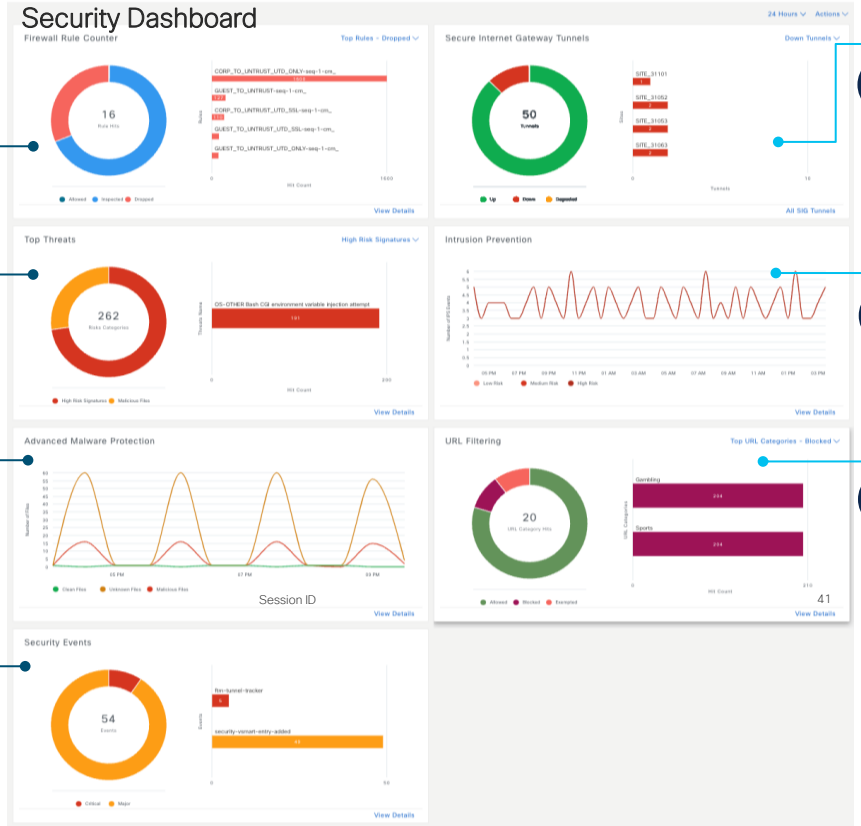


1. Cisco Secure Access establishes a secure connection with ISE context-services to consume SGTs
2. Learned SGTs can be leveraged to define access policies for branch accessing Internet/SaaS applications
3. In Catalyst Manager the Secure Service Edge policy group is configured to share SGT context in tunnels
4. Once tunnels are up, SGT identities, learned from enterprise are shared inline in the IPsec meta data header towards Cisco Secure Access.
5. Packets with SGT ID context are then subject to SSE policy match as source objects in the
6. SGT to IP Mapping can be learn both using inline or using OOB catalyst SD-WAN Manager ISE integration. Inline tag preferred over OOB.
7. Both VPN and SGT can be shared together

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Management and Reporting

SD-WAN manager SecOps dashboard



1 **Firewall Rule counter**
Overview of top rule hits within network with an ability to drill down to individual device level

2 **Top Threats**
Overview of the critical threats (IPS/AMP) in the network

3 **Advanced Malware Protection**
Trend of incoming files in the network. Categorized into clean, unknown and malicious

4 **Security Events**
Displays raw events captured in the network

5 **Secure Service Edge (Cisco Catalyst SD-WAN secure internet gateway – SIG)**
Provides the status of each SIG tunnel hosted by the SD-WAN routers

6 **Intrusion Prevention**
Trend of IPS events in the network with an ability to view event details and associated devices

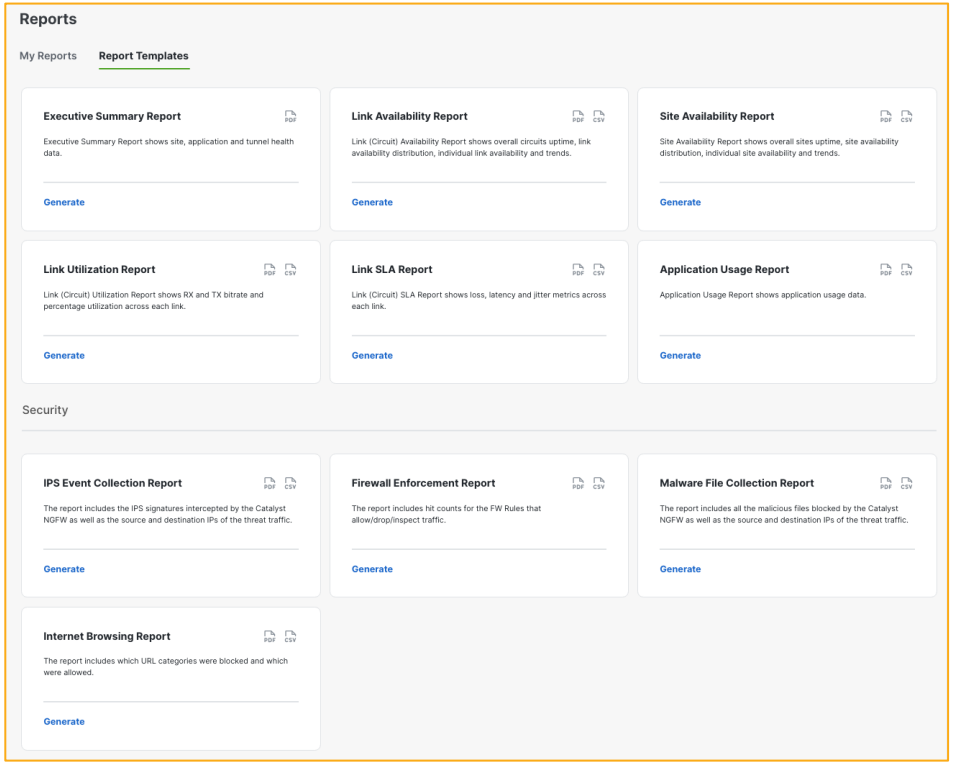
7 **URL Filtering**
Displays web categories accessed by the user

Customers can customize the dash-let on this security dashboard

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

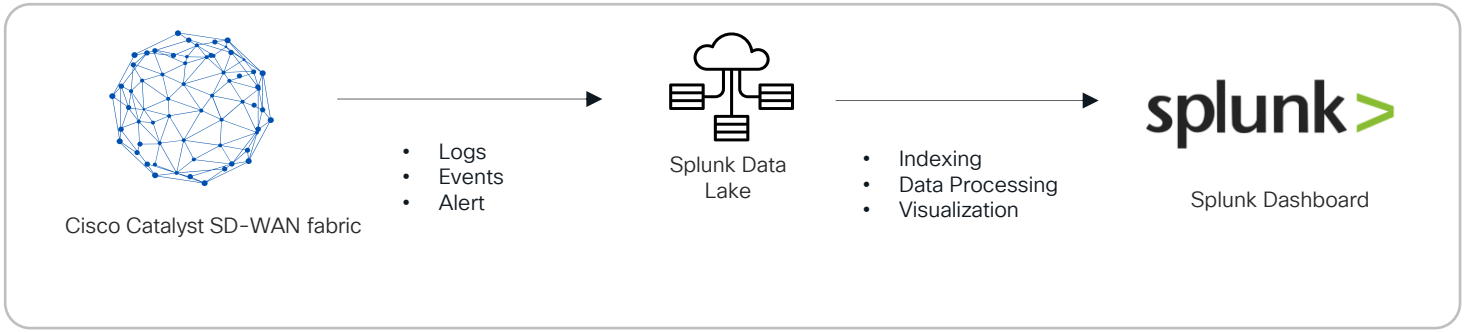
Catalyst SD-WAN Manager Security Reports

- Configuration workflow for generating security-related reports is the same as configuring for site, tunnel, application, etc..
- Reports can be generated in either PDF or CSV format.
- Security reports can also be generated at a recurring interval with the option of email delivery.



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Catalyst SD-WAN & Splunk integration



SoC Dashboard

- Holistic view of all security events
  - Top Threats & Policy Hits
  - Overall Application Traffic
- Drill down to device level from any security widget (user/sgt)

Flow Analysis

- View device network patterns
- Top applications accessed
- Top website domains visited
- Generate reports

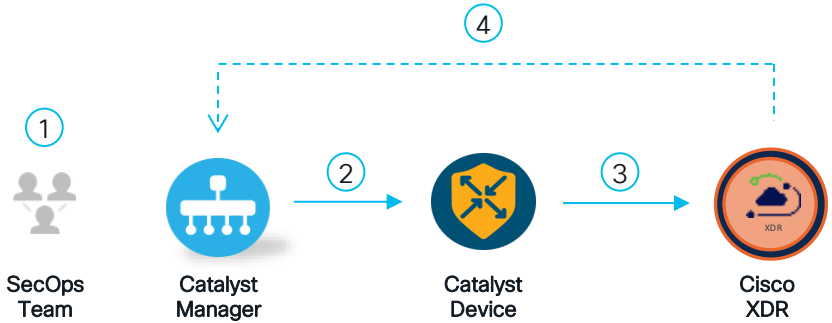
Threat Management

- List all IPS events in the network
- List all Malware events in the network
- View which devices are impacted by threat events

App URL: https://splunkbase.splunk.com/app/6657 App Add-on: https://splunkbase.splunk.com/app/6656 HSL Add-on: https://splunkbase.splunk.com/app/6872

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco eXtended Detection and Response (XDR)



Customer Journey

1. Purchase single SKU
2. Initiate workflow from Manager
3. Threat Incident analysis & correlation
4. Visualize analytics on Manager

Event Correlation

- Collect Telemetry from WAN, LAN and endpoints
- Correlate security events

Anomaly Detection

- Establish baseline for user/device behavior
- Detect anomalies and malicious events

Threat Remediation

- Security Incident creation
- Automatic threat remediation using AIOps

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Microsoft Sentinel – SD-WAN security visualization

Comprehensive Visibility

- Visualize SD-WAN Security events
- Comb through Firewall rule data
- Drill down to device, user and flow levels

Microsoft Azure Fabric

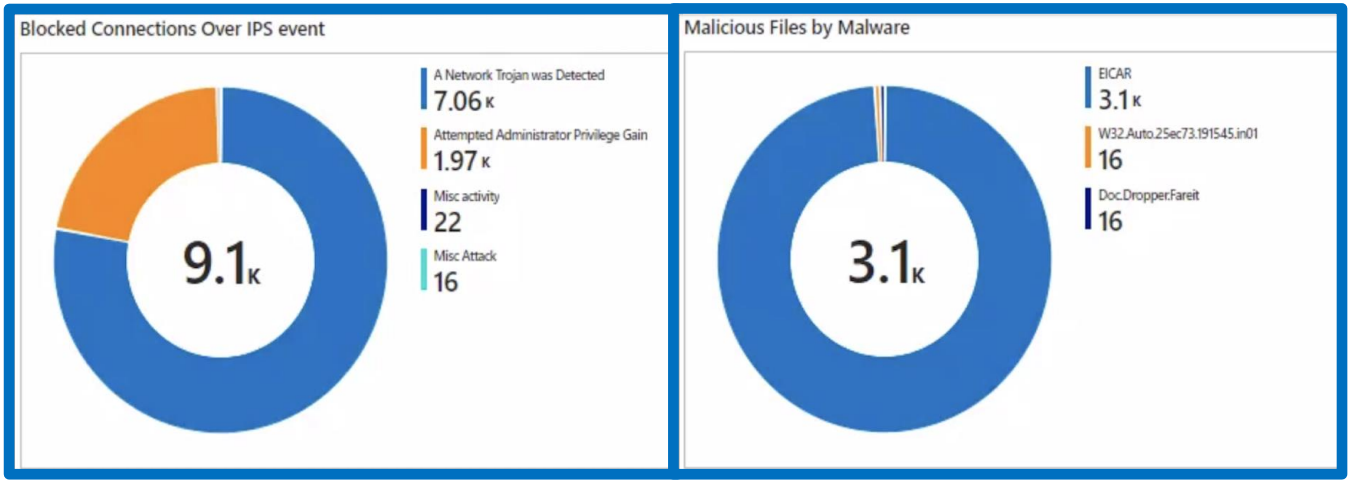
- Strong Cisco / Microsoft Partnership
- 100+ customers already use Azure fabric
- Interconnect other MSFT Services

Act on the Threats

- Threat Hunting
- Execute Playbooks
- Analyze threats based on MITRE ATT&CK framework

Asset Protection

- Visualize threat events captured by the SD-WAN Security Stack
- Comb through Intrusion attempts to your network entities
- Parse through all the malicious files captured in your network



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco Live!

Keynote Deep Dives

Wednesday
10:30am –11:30am

Experiences Amplified: How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106

Smart, Secure, Seamless: Transforming Experiences with Next-Generation Networking

Level 2
Room 204

Harness a Bold New Era: Transform Data Centre and Service Provider Connectivity

Level 2
Room 203

Securing User to Application and Everything in Between

Level 2
Melbourne Room 2

Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.

Complete your surveys in the **Cisco Live mobile app**.

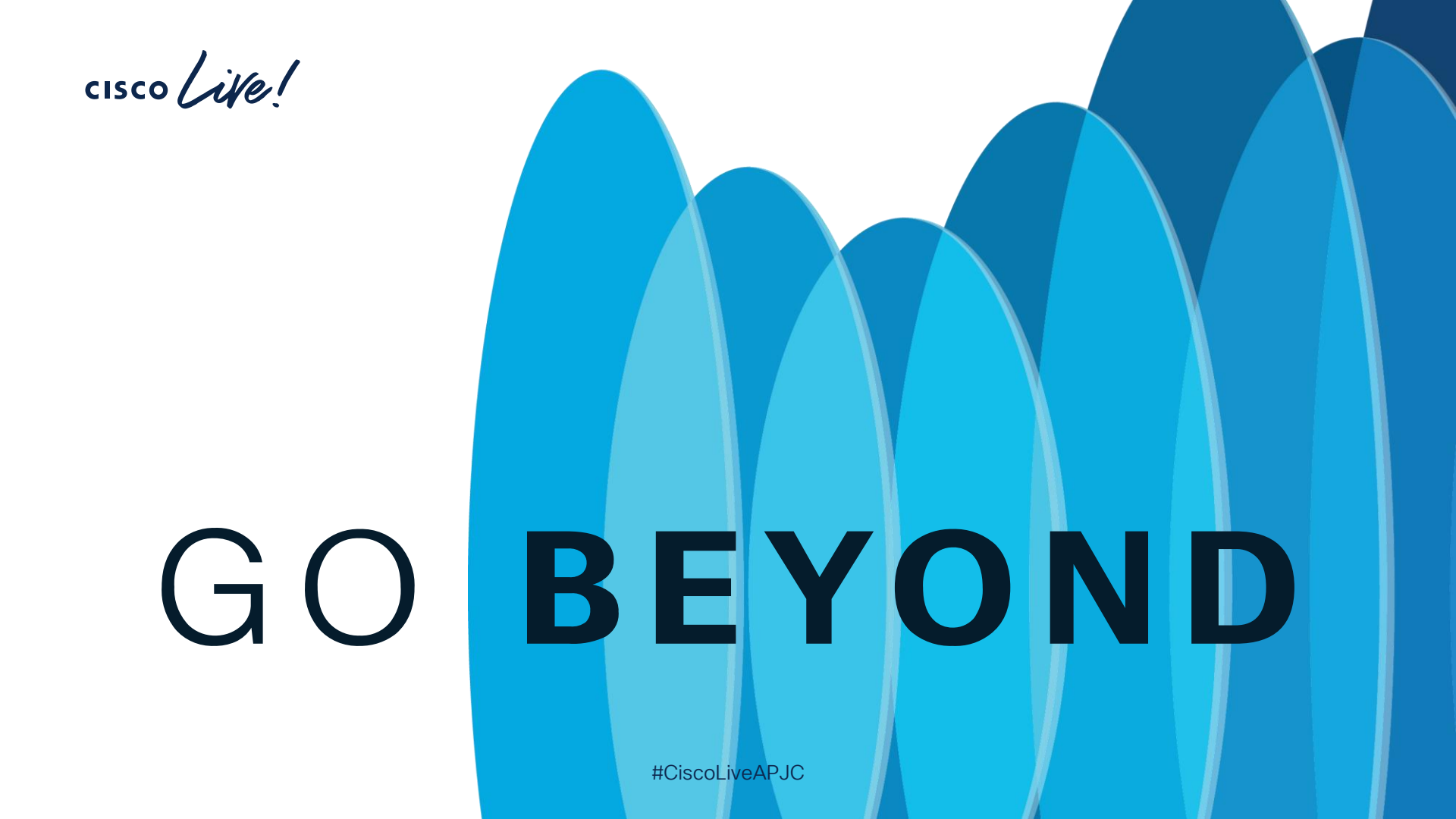
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco
Thank you
cisco Live!
#CiscoLiveAPJC


cisco Live!
GO BEYOND
#CiscoLiveAPJC