Cisco IT Tetration Deployment, Part 2 of 2

This white paper is one in a series of case studies that explain how Cisco IT deployed ACI to deliver improved business performance. These in-depth case studies cover the Cisco IT ACI data center design, migration to ACI, the ACI NetApp storage area network deployment, compute at scale with AVS, UCS, KVM, and VMware, server load balancing, Tetration analytics (parts 1 and 2), and ACI OpenStack automation, and Network Assurance Engine. These white papers will enable field engineers and customer IT architects to assess the product, plan deployments, and exploit its application centric properties to flexibly deploy and manage robust highly scalable integrated data center and network resources.

Contributors to this white paper from the Cisco IT include Ben Kelly, Network Architect, Benny Van De Voorde, Principal Engineer.

Version: 1.1, June 2020 – updated with copy edits for clarity.

Americas Headquarters

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

http://www.cisco.com

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883

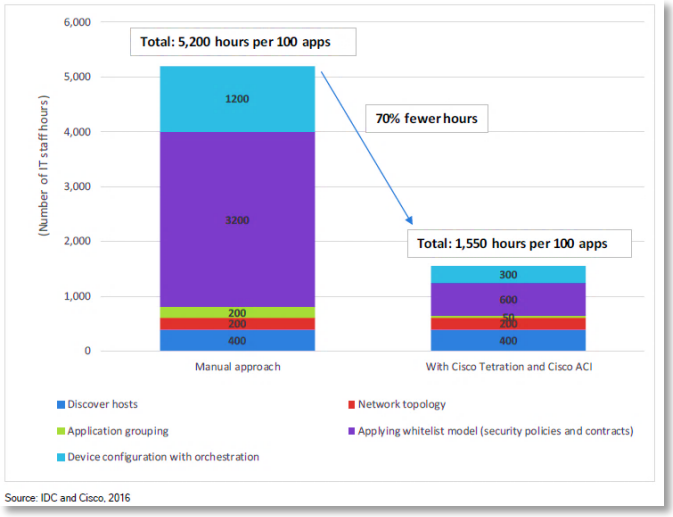
Table of Contents

Cisco IT Tetration Deployment with ACI, Part 2 of 2

Cisco IT data center environment deploys thousands of applications that support the enterprise, its partners, and customers. Cisco ACI technology easily provides great value in automating operations of classical networking processes. Cisco ACI enables Cisco IT to use a common application-aware policy-based operating model across their entire physical and virtual environments.

Applications are guiding the design of data center infrastructure. Today's applications are dynamic, using virtualization, containerization, microservices, and workload mobility technologies, with communication patterns between application components constantly changing. Now, 76 percent of data center traffic is east-west, a fundamental change from traffic patterns in the past. This technological shift has contributed to an increased attack surface and free lateral movement within the data center infrastructure. The Cisco Tetration™ platform addresses data center operational and security challenges by providing comprehensive workload-protection capability and unprecedented insights across a multicloud infrastructure. As Ben Kelly, Cisco IT Network Architect, says, "There is simply no other way to perform application dependency mapping, policy enforcement, and workload protection in large scale data centers as effectively."

According to an IDC white paper, Cisco achieved a 70% reduction in staff time required to



gain insight into application behavior.

Staff Time Needed for Application Dependency Mapping, Tetration Versus Manual Approach

A subsequent IDC white paper validated the Tetration platform approach for holistic workload protection.

The result is that Cisco IT can not only be more agile in delivering scalable high performance on premises data center services but also more quickly and fully achieve the business intent of the organization.

With Cisco Tetration and Cisco ACI, Cisco IT can provide much higher value to the enterprise by cost effectively performing the functions at scale that were previously not feasible. This is the second of two white papers that show exactly how this is possible. This second paper covers how Cisco IT deployed the following Tetration capabilities:

- Enhanced security and access agility design based on deploying scopes, RBAC, ACI security policies along with other security mechanisms such as WAF, IDF, and encryption.
- Simulate policy for impact analysis
- Policy compliance audit
- Forensic analysis with replay of historical full flows

Cisco Tetration v3

The Cisco Tetration™ platform is designed to fully address data center operational and security challenges using comprehensive traffic telemetry data collected from both servers and Cisco Nexus® switches. Cisco Tetration offers holistic workload protection for multicloud data centers by enabling a zero-trust model using segmentation. This approach allows you to identify security incidents faster, contain lateral movement, and reduce your attack surface. Tetration's infrastructure-agnostic approach supports both on-premises and public cloud workloads. The platform performs advanced analytics using an algorithmic approach and provides comprehensive workload protection for a multicloud data center. This algorithmic approach includes unsupervised machine-learning techniques and behavioral analysis.

Cisco Tetration use cases

The Cisco Tetration platform supports these critical data center security and operations use cases:

- **Workload protection:** Enables holistic workload protection for multicloud data centers. Segmentation based on only allowing specified traffic enables implementation of a zero-trust model.
- **Identify process behavior deviations and detect software vulnerabilities:** Baseline the behavior of the processes running on servers. Identify behavior deviations matching malware-style execution. Detect latest events such as Spectre and Meltdown. Get an accurate inventory of all software packages and version information installed on servers. Detect whether any packages have known CVEs and define specific remediation.
- **Network Insights:** Robust data-plane telemetry information from servers and the network, in conjunction with machine learning, enables the Cisco Tetration platform to provide better network and flow performance insights to the operations team.
- **Control user access to applications:** Collect telemetry data from end points through Cisco Any connect. Enhance segmentation policy to restrict application access using user and user group information.
- **Security dashboard**: a composite security score for workloads based on various parameters, including policy compliance events, vulnerabilities identified, and process behavior consistencies. Quickly identify workloads with behavior deviations and see compliance score for applications.

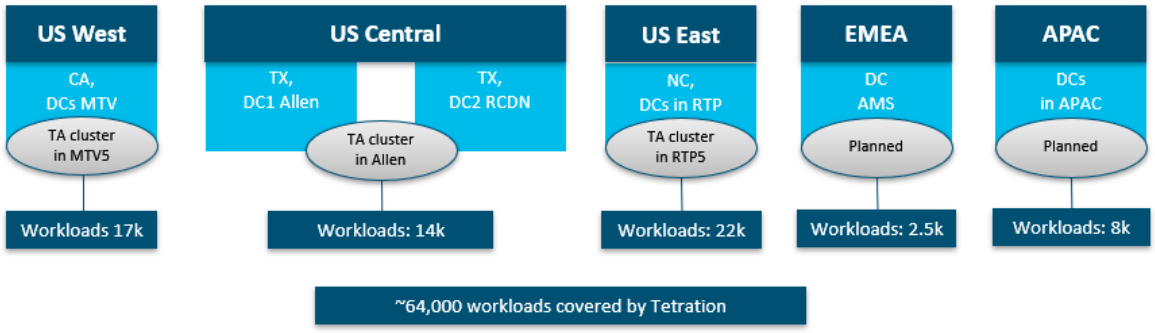
Multidimensional workload protection approach using Cisco Tetration

By using this multidimensional workload protection approach, Cisco Tetration significantly reduces the attack surface, minimizes lateral movement in case of security incidents, and quickly identifies anomalous behaviors within the data center.

Cisco IT Tetration Deployment Case Study

The Tetration platform can be deployed on-premise in two form factors, and in the public cloud, such as Amazon Web Services. The current and target Cisco IT deployments use the Tetration on premise options, as illustrated in the following figure.

Cisco IT Tetration Deployments



Cisco IT installs Tetration agents on hosts that are in their roadmap for migration to ACI. Currently, Cisco IT has 3 Tetration clusters deployed using hardware sensors in -EX versions of their Nexus 9000 switches, and over 28,000 agents, with an additional 20,000

agents in their roadmap. For both scalability and resiliency, all Cisco IT Tetration clusters are the large form factor hardware option.

By using software sensors, hardware sensors, and Encapsulated Remote Switched Port Analyzer (ERSPAN) sensors across the data center infrastructure, the Tetration platform can support both existing (brownfield) and new (greenfield) deployments. Software sensors also act as enforcement points for application segmentation. Tetration is powered by big-data technologies that support data center scale. It processes comprehensive telemetry information received from sensors in near-real time (up to 2 million telemetry events per second). The platform enforces consistent policy across thousands of applications running on tens of thousands of servers. It is also designed for long-term data retention; it can search tens of billions of telemetry records from its data lake and return actionable insights in less than a second.

Tetration Automated Inventory Cataloguing with Custom Tags

Tetration uses machine learning to offer inventory cataloguing with custom tags, network analysis, application dependency mapping, and security enforcement features that are only possible when paired with its full flow comprehensive data set. The custom tag annotation capability enables Cisco IT to visualize and define policies using consistent attributes across its environment.

Cisco Tetration Automated Inventory Cataloging

- **Agent feed with custom tags**: discovers inventory based on all nodes observed on the network directly via agents/ASICs (including vCenter and AWS virtual machine attributes), or indirectly via a flow to or from an agent/ASIC, merges with uploaded inventory - for example, from a configuration management database - and custom metadata tags.

- **Inventory tracked**: in real time along with historical trends.

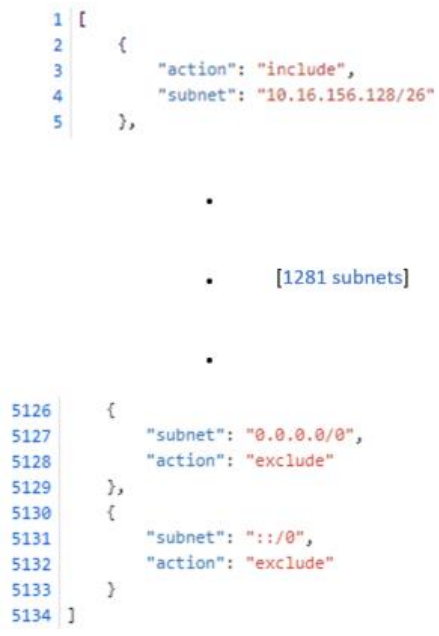
Inventory includes both internal and external hosts. An internal host is a host running a software agent or included in the Tetration collection rules. An external host is any other host with traffic observed on the network. Inventory access can be restricted by scope and RBAC rules.

Endpoint Inventory, User Annotations, and Inventory Collection Rules

All IP addresses that the Tetration cluster can see via network flows are added into the inventory, according to the collection rules.

The following figure illustrates a snippet of the Cisco IT JSON file that contains its Tetration collection rules:

File snippet of the Cisco IT JSON Tetration collection rules



Tetration collection rules catalog which endpoints seen in flow data are to be added to the inventory. The Cisco Tetration product team recommends keeping the total inventory under 1 million end points. Cisco IT Tetration clusters are limited such that only data center hosts are covered (around 400,000 hosts), which keeps the inventory well under this number.

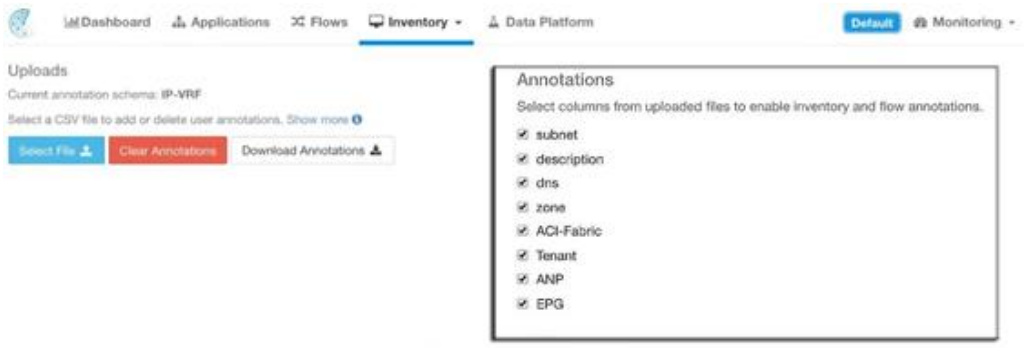
Endpoints in the inventory can have user defined tags associated with them. These tags are known as user annotations and can be used to group hosts and apply security policy rules. Tetration allows annotations for up to 1.5 million IPv4/IPv6 addresses and 30 thousand IPv4/IPv6 subnets per root scope. These limits are well above the maximum that Cisco IT expects to require.

The population of the tags required for scope definition within Tetration are loaded into the platform. User uploaded tags with annotations for inventories enable observing the network in the known familiar terms of an enterprise. The data itself is pulled from the Cisco IT ACI fabrics, ServiceNow, and IP address management databases. This process is automated.

User Tags Currently in Use

User Tag Name (Annotation)	Description
aci_fabric	ACI Fabric
aci_tenant	ACI Tenant
aci_ap	ACI Application Profile
aci_epg	ACI End Point Group
dns	DNS Hostname
host_lifecycle	Lifecycle of host (dev, stg, prod)
host_priority	Host Priority (P1-P6)
network_zone	Network Security Zone (internal, DMZ)
support_group	Host team support alias

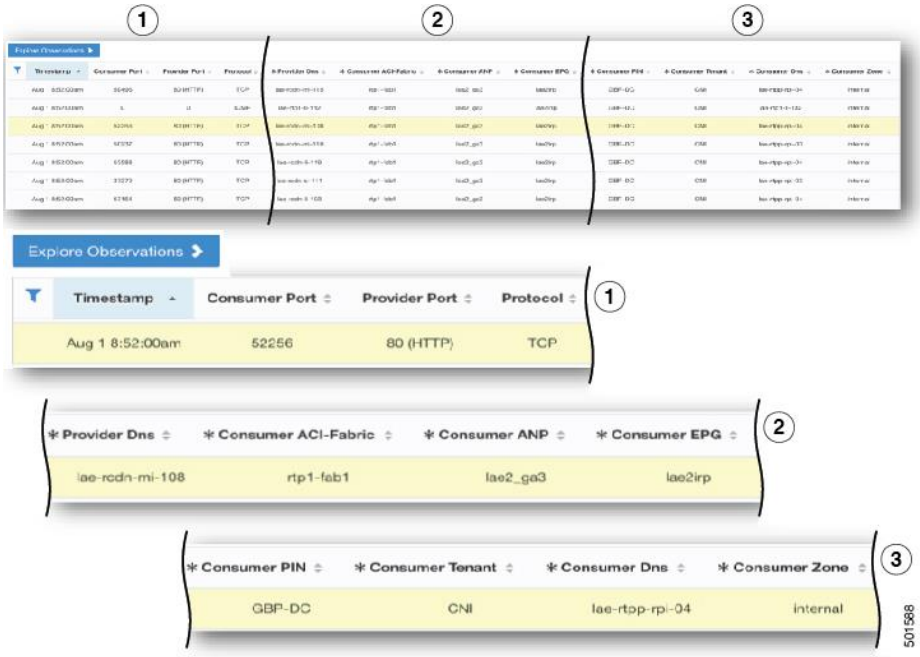
A Sample of Cisco IT Inventory Cataloging with Custom Tagging Annotations



In this example, Cisco IT used python scripts to upload to Tetration CSV tables containing categories of items that included subnets, descriptions, DNS servers, zones, ACI fabrics, tenants, application profiles, and EPGs.

The result is that query tables display the results using labels Cisco IT uploaded to Tetration. As shown in the illustration below, this makes for a much easier to read and understand set of information.

A Sample Query Result Showing Cisco IT Inventory Cataloging with Custom Tag Annotations



Portion 1 of this illustration shows the columns Tetration provides. Portions 2 and 3 of this illustration show asterisks next to the column names which indicates that they are categories of information Cisco IT customized within Tetration. As you can see, the query result table uses the naming conventions of the Cisco IT data center.

Moreover, custom inventory tag annotations provide additional identifiers for discovered endpoints. Inventory query filters can match many identifiers that are provided to Tetration.

Examples of Cisco IT Inventory Filters

Item	Cisco IT Naming Standard
Address Space	All Networks
DMZ Address Space	All DMZ Networks
Internet	Internet (0/0)
Enterprise Management	Infra Service – Enterprise Management
ServiceNow Networks	Infra Service - ServiceNow
Infosec Networks	Infra Service - Infosec
Privileged Access Management	Infra Service - TPAM (Priv Access)
NTP	Infra Service - NTP
TACACS+	Infra Service - TACACS
SMTP	Infra Service - SMTP
DNS	Infra Service - DNS
Directory Services Prod	Infra Service - Directory Services (Prod)
Directory Services nProd	Infra Service - Directory Services (nProd)
OS Infra	Infra Service - OS Infrastructure Services
Storage Internal	Infra Service - Storage (Internal)

For example, an endpoint can have an identifier that specifies it is a production or non-production workload, PCI or HIPPA, or its network zone. An inventory query filter that finds all production workloads enables easily creating a policy that strictly enforces prevention of production workloads from communicating with non-production workloads.

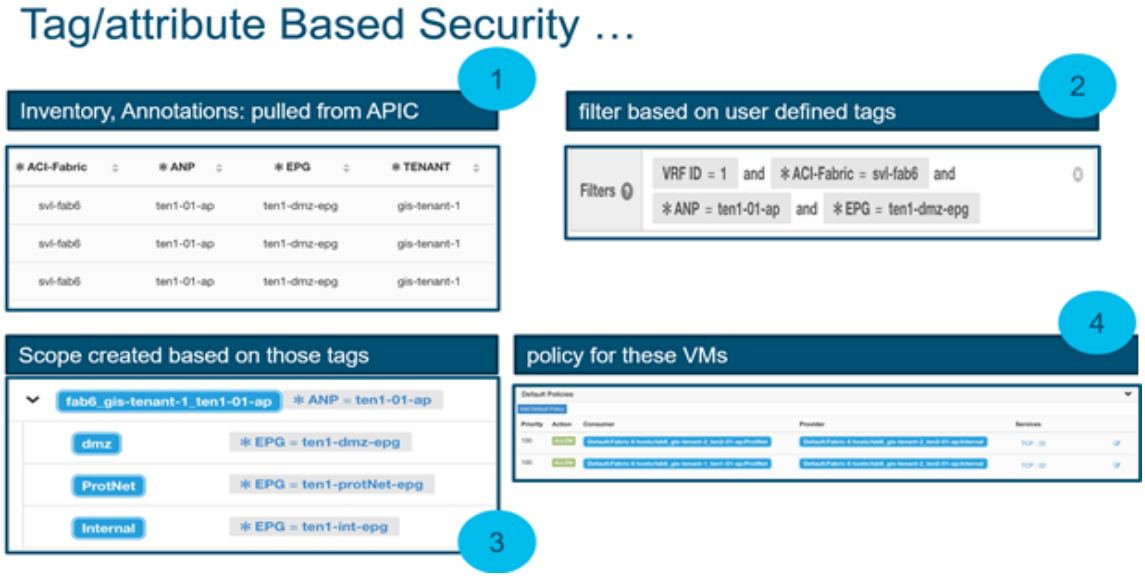
Generating a Tag/Attribute Based Security Policy

Tetration provides scope and Role Based Access Control (RBAC) access control. Scopes

are hierarchically organized groups of assets/endpoints to which role abilities (read, write, execute, enforce, owner) rules and RBAC access control (including Active Directory) can be applied.

Cisco IT has designed a tag/attribute-based security model it will deploy in Tetration to enhance the security of its ACI data center operations.

Cisco IT Tetration tag/attribute security model



1. Cisco IT uploaded custom inventory tag attributes to Tetration. One of the custom inventory tags Cisco IT uploaded to Tetration is ACI application network profile (ANP).
2. Now, they can use Tetration to create a filter that identifies a particular ACI application profile in its data center.
3. Based on that filter, they create a scope that includes those tagged items.
4. Finally, they establish ACI security policies with contracts and appropriate ACI filters.

Tetration Scopes

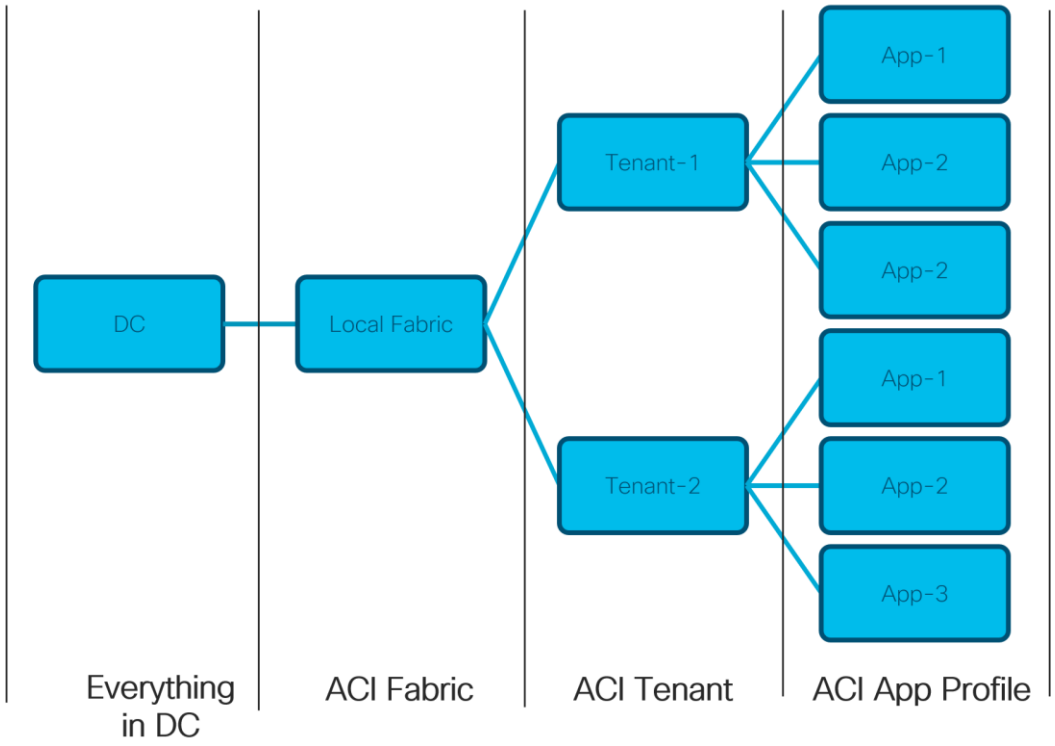
Tetration uses scopes to group end points into the following categories:

1. User has visibility and control
2. Enforced application workspace (more details below).

Scopes are arranged into a hierarchy. The Cisco IT implementation leverages a scope hierarchy 4 levels deep.

- Default: All IP addresses – everything in the data center
- Local Fabric: All IP addresses in a particular data center fabric
- Tenant – An ACI tenant
- Application Profile - An ACI application profile

Tetration Analytics Scope Hierarchy



Tetration Role Based Access Control

Tetration roles are made up of capabilities that include a Scope and an Ability. These define the allowed actions and the set of data they apply to. For example, the (HR, Read) capability should be read and interpreted as "Read ability on the HR scope". This capability would allow access to the HR scope and all its children.

Ability	Description
Read	Read all data including flows, application and inventory filters.
Write	Make changes to applications and inventory filters.
Execute	Perform ADM runs and publish policies for analysis.
Developer	Access to Data Platform features such as creating and running User Apps, scheduling Jobs, and uploading data to the Data Lake. See Data Platform for full list of Developer abilities.
Enforce	Enforce policies defined in application workspaces associated with the given scope.
Owner	Required to toggle an application workspace from secondary to primary. Access to Data Platform Admin abilities such as managing User App sessions, adding Data Taps, and creating Visualization Data Sources (see Data Platform).

The Cisco GIS DC networking team owns the enterprise Tetration solution. However, other groups require access to Tetration, its API and GUI. Cisco users who need access to Tetration fall into two main groups:

- **Infrastructure Admins**: have full access to Tetration. This includes the Infosec team
- **Application Owners**: have access to just their applications within Tetration

There are subgroups in each of the above, divided into those who need read/write access and those who only require read only access.

The above roles are assigned to these Cisco IT specified scopes:

- Default Scope Level: Infrastructure admins
- App Profile Scope Level: Application owners

Cisco IT maps users to roles based on the LDAP group membership via an SSL enabled connection between the Tetration and LDAP clusters.

Cisco IT Data Center Policy Enforcement

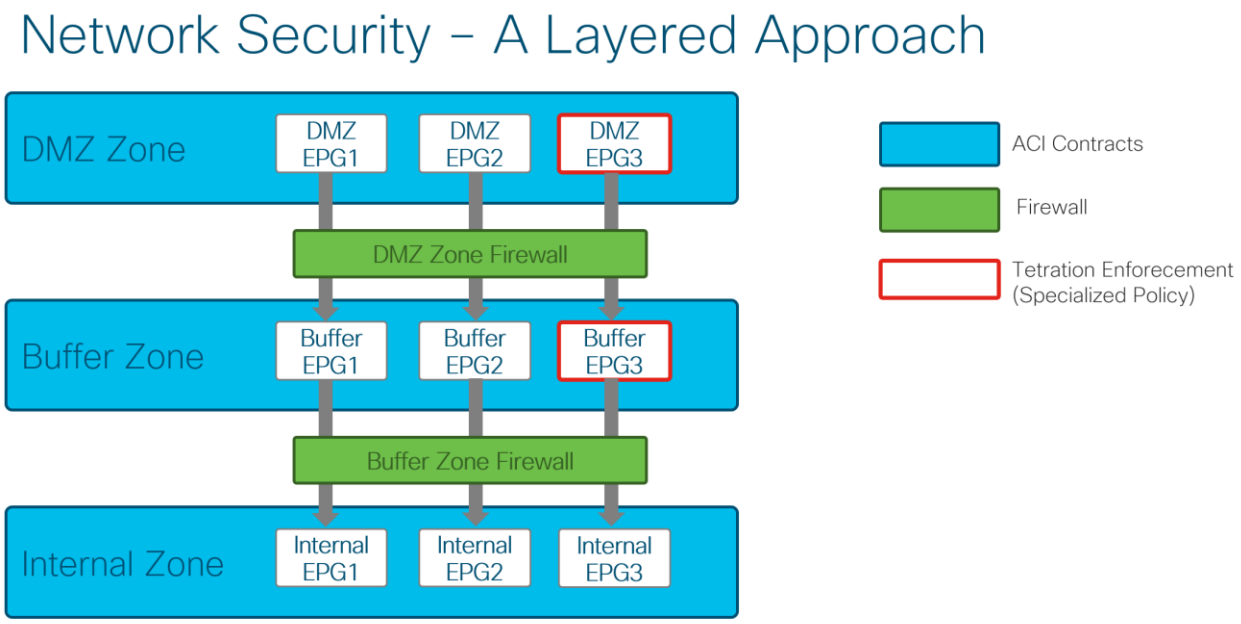
Cisco IT has a multi-layered approach to network policy enforcement and developed the following design. The enforcement of network security policy is achieved with three technologies:

- Stateful firewalls – For securing traffic between security zones (e.g.: DMZ to internal)
- ACI security contracts - For traffic within a particular security zone
- Tetration Analytics enforcement - For applications with specialized security needs

With these building blocks in place, Cisco IT designed a layered approach to data center security that provides greater agility and enhanced security to the Cisco enterprise.

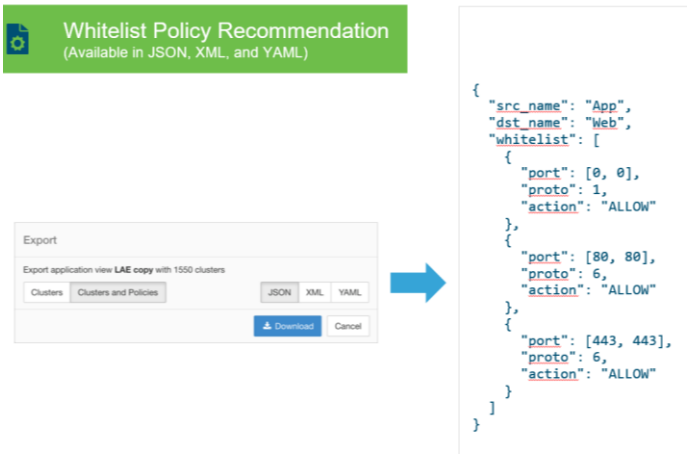
When it comes to data center networking security, Tetration gives Cisco IT the visibility of all the flows that need to happen within any portion of the data center. This visibility enables analysis and enforcement of security in different ways according to whatever the security requirements might be. Cisco IT security requirements determine what they will enforce with any given technology.

Cisco IT multi-layered data center networking security



Using ACI contracts, Tetration, RBAC, and mandated firewall rules, Cisco IT greatly enhances their security posture which already includes web application firewall (WAF), intrusion detection systems (IDS), and encryption (both standing and in transit). Tetration can provide granular analysis of policy changes which enhances compliance related notifications.

Cisco Tetration Policy Deployment



While the example of an auto-generated policy illustrated here is small, an actual Cisco IT Tetration auto-generated security policy could have thousands of lines. Cisco IT takes that policy and deploys the relevant portions of it in multiple areas of its ACI data center

infrastructure, such as ACI contracts enforced in the switches, firewall policies, and in the Tetration host agents that enforce the policy as well.

For example, if there is an ACI EPG running in the DMZ VRF that needs to communicate with an EPG in the internal VRF, then it must go through a firewall. In addition, Cisco IT can specify granular and specialized security requirements that the Tetration agent will enforce in the hosts themselves.

Enforcement Workspaces and Policy Enforcement Priority

For those users who need fine-grained security, Cisco IT can enable the following access capabilities:

- Application owners have a level of autonomy to make application level changes quickly.
- Security and network teams control the global aspects of application inter-connection and shared services.

Tetration Analytics uses the concept of application workspaces to provide views into a particular scope (i.e.: set of hosts) as well as the configuration of network security policy. Multiple workspaces can be used for any given scope, however only one workspace per scope can be used to enforce policy. Although it is technically possible to have policy enforcement at each level of the hierarchy, to keep the solution easy to understand, configure and troubleshoot, Cisco IT has elected to enforce policy only at the Local Fabric and EPG levels of scope hierarchy.

Cisco IT divided the policy enforced at the different scopes into these two levels:

- Broad level local fabric level services (infra) - Infrastructure (DNS, NTP, etc.) and Foundation (OAM, MMX, etc.)
- Application specific EPG level - client specific configuration requirements

Tetration Analytics uses a priority order with which to determine which polices in which enforcement workspaces to apply. A workspace scope with a lower number assigned is considered a higher priority. Each enforcement workspace has two types of network security policies - absolute and default. Lastly, each workspace also has a catch all policy which can be set to either ALLOW or DENY.

The example below illustrates the order in which policy is applied. Three scopes with the following policy priority order:

1. Apps
2. Apps:HR
3. Apps:Commerce

Each of the above scopes have at most one primary application workspace with absolute policies, default policies and a catch-all action. Each group of absolute or default policies within each application workspace is sorted according their local priorities.

The ordering of the policies will be as follows:

1. Apps Absolute policies
2. Apps:HR Absolute policies
3. Apps:Commerce Absolute policies
4. Apps:Commerce Default policies
5. Apps:HR Default policies
6. Apps Default policies
7. Apps:Commerce Catch-all
8. Apps:HR Catch-all
9. Apps Catch-all

Absolute policies are first evaluated top to bottom. Next, default policies are evaluated bottom to top. Lastly, catch-alls are evaluated bottom to top

Global Level Policies

Cisco IT "Infrastructure" services are permitted using absolute policies in the 'Default' scope (i.e.: global level). This scope also is set to the lower scope priority number, meaning that the absolute policies are evaluated first and the default policies last:

- Enterprise Management
- Infosec Networks
- Privileged Access Management
- NTP
- TACACS

- SMTP
- DNS
- Directory Services
- NTP
- Operating Systems Infra

Since these absolute policies are evaluated first, they apply to all endpoints in that local fabric and cannot be overridden by application workspaces lower in the hierarchy.

Application Level Policies

Each application has its own enforcement workspace. Application owners have access to configure their own absolute or default policies in this workspace. Should an application owner determine that hosts within their workspace needs to communicate to a host in another workspace, they can set the provider/consumer for that policy to the other scope. In this way it works very much like a contract between EPGs in the ACI policy model.

Note how policies between workspaces operate. Take two workspaces:

- App1
- App2

If a policy is created in App1, where a service is provided from App2, then a policy request is created in App2. The policy will become active until the admin of App2 accepts the policy request.

Providing/Consuming Services Between Scopes

It is possible to set up "auto-pilot" rules within a workspace to automatically accept requests to provide services to other scopes. These can be set to just particular protocols/ports or accepting all.

Policy Filters

Policies and filters in a workspace can identify EPG providers/consumers for particular network flows. Filters match endpoints and can use attributes such as IP address, hostname, custom tag or combinations of those. The Cisco IT infrastructure team created a set of standard filters in the default scope that are used in any workspace. These pre-defined filters cover broad network types and common use cases:

- Standard Address Blocks
- Cisco address space (all)
- Cisco DMZ space (all)
- Internet
- Standard Infrastructure
- Enterprise Management
- Infosec
- Privileged Access Management
- NTP
- TACACS
- SMTP

- DNS
- Directory Services
- NTP
- Operating System Infra
- Oracle Access Manager
- Oracle Connection Manager
- Web Services Gateway (external)
- Web Services Gateway (internal)
- Middleware Messaging
- Storage

In addition to these Cisco IT has also created filters which match EPGs within data center ACI fabrics. All the EPGs are replicated as Tetration filters. This enables easier configuration of applications and aligns the same group of EPG hosts in the fabric with the same group of hosts in Tetration. This alignment means grouping of hosts between ACI and Tetration is the same and therefore policy is more consistent.

If a client requires their own filters, those are created in the app profile level scope and are configured and named as the client wants. The filter is only visible with that scope and below and avoids clutter in other scopes.

Windows Advanced Firewall

On Windows OS systems, the Tetration agent programs the Windows Advanced Firewall to enforce the specified security policy. The rule order is determined by limitations of Windows Advanced Firewall is summarized in the table below. It may not match what is configured in the Tetration workspace.

Table: Windows Advanced Firewall Rule Order

Order	Rule type	Description*
1	Windows Service Hardening	This type of rule restricts services from establishing connections. Service restrictions are configured by default so that Windows Services can only communicate in specific ways (i.e., restricting allowable traffic through a specific port) but until you create a firewall rule, traffic is not allowed. Independent software vendors can make use of public Windows Service Hardening APIs to restrict their own services.
2	Connection security rules	This type of rule defines how and in which circumstances computers authenticate using IPsec. Connection security rules are used in establishing server and domain isolation, as well as in enforcing Network Access Protection (NAP) policy.
3	Authenticated bypass rules	This type of rule allows the connection of computers if the traffic is protected with IPsec, regardless of other inbound rules in place. Specified computers can bypass inbound rules that block traffic: examples of this are vulnerability scanners, programs that scan other programs, computers, and networks for weaknesses.
4	Block rules	This type of rule explicitly blocks a particular type of incoming or outgoing traffic.
5	Allow rules	This type of rule explicitly allows a particular type of incoming or outgoing traffic.
6	Default rules	These rules define the action that takes place when a connection does not meet any of the parameters of a higher order rule. Out-of-the-box, the inbound default is to block connections, and the outbound default is to allow connections.

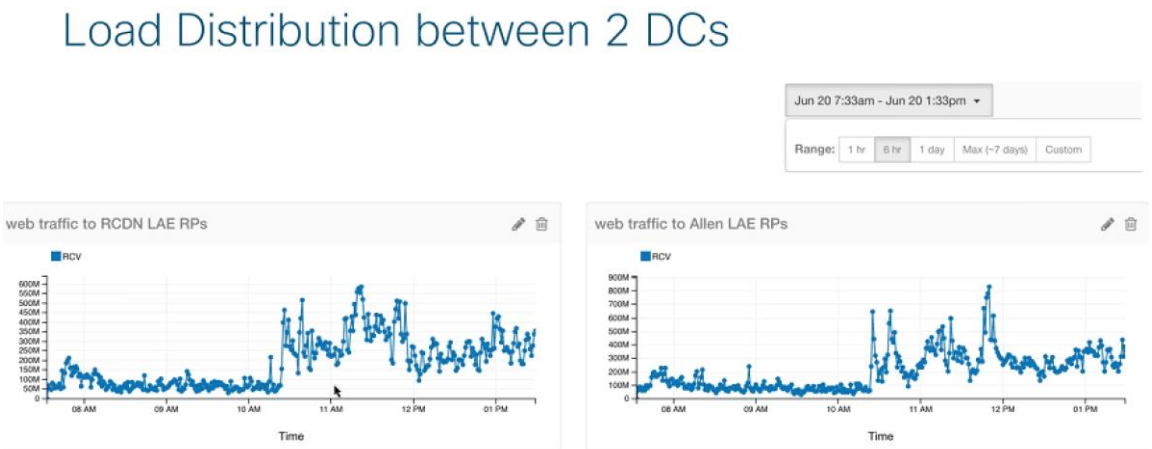
* More details about Windows Advanced Firewall can be found here.

Dashboard

The dashboard presents graphical views of Tetration data, which you can customize according to requirements for tasks such as monitoring, incident resolution, or forensics. The Tetration data platform enables running various logic within Tetration such as simple SQL queries to get filtered data to monitor network flows. The data platform also provides the capability to bring your own data streams into Tetration, using a framework that integrates external data with Tetration applications to visualize the data in the Tetration GUI or send notifications to northbound systems. These two features can aid in quickly assessing actionable insights from Tetration.

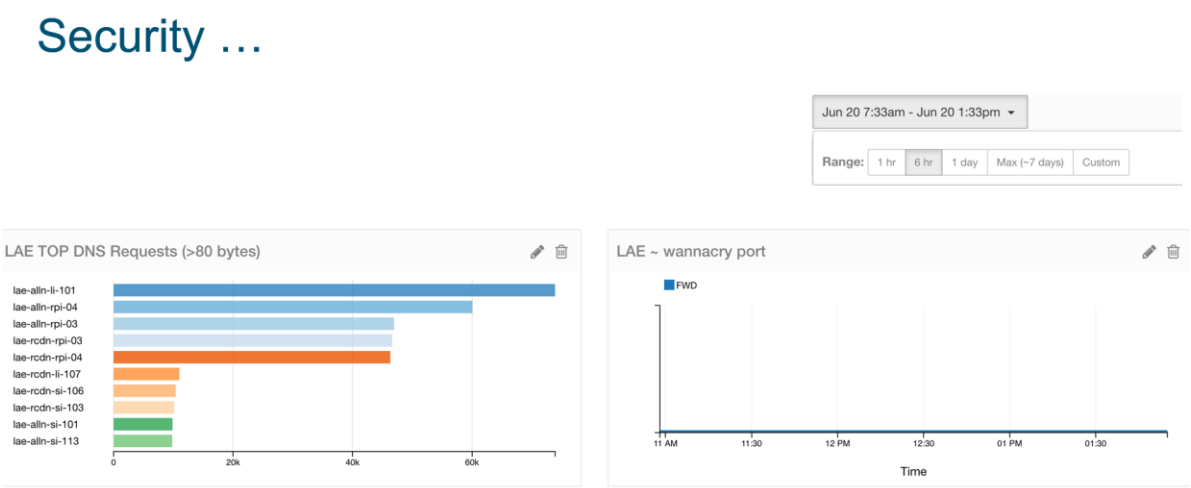
Cisco IT uses Tetration to monitor application performance and deviations. The Cisco IT Lightweight Application Environment (LAE) is the platform as a service (PaaS) environment that provides operating system, middleware, and system functions as services. Cisco IT monitors its LAE application for a variety of reasons, including proactively assuring service level agreements are met. LAE is deployed in an active/active mode across the Richardson Texas and Allen Texas data centers.

Example of dashboard view of the Cisco IT LAE application traffic



The Tetration dashboard shows the relative distribution of the load across both data centers. The normal case is for the workload to be distributed evenly across both data centers. If Cisco IT operations sees that one data center has a very low workload, they would suspect a problem exists that must be addressed before there is a disruption in the operation of the LAE application.

Example of dashboard view of the Cisco IT LAE application DNS requests



Another example of a dashboard filter on the LAE application shows detailed DNS request information. Furthermore, Cisco IT used another query with specific filters that identify a WannaCry DNS attack.

The results of user created routines that extract actionable data from Tetration automatically can be handed off to other systems such as monitors or for reporting, further investigation, or compliance audits. For example, application latency can be monitored vs. Smoothed Round Trip Time (SRTT) latency for various servers. In Tetration, you can specify if you want to see any network flow taking more SRTT and you can add multiple filters (for example, host names, port, protocol). A simple SQL query could be written to pull the filtered data from Tetration to monitor the network flow. Then, if the SRTT SLA value is over 90 ms, the Tetration open APIs enable using scripts that easily and automatically push an alert to a monitoring system.

A dashboard for network operations and infosec to see the current overall status of TA agents with statistics, such as

- Total number of agents
- Number of non-compliant agents
- List of non-complaint agents, in order of criticality
- Agents which will soon be considered non-compliant (i.e.: time they've been offline is about to go over threshold)

- Status of the automation software that creates the report (i.e.: when it last ran, how long it took)

The dashboard also stores the agent status reports for historical tracking.

Cisco IT Network Policy Approval Workflow

In the Cisco security model, application owners who leverage Tetration enforcement have a much more direct involvement in the configuration of the security policy for their application/service. A change to network security configuration must be appropriately tracked and go through an approval workflow.

The infosec group mandated that a change in network security configuration must generate a support case. Some changes requested by the client (or infrastructure admin) can be auto approved and pushed out immediately.

Changes that do not meet the criteria for auto-approval must be reviewed by infosec. They have the option to approve or reject the request.

High level summary of a Cisco IT basic approval process is listed below:

1. Client makes a network security policy change request
2. Support case is automatically generated
3. Notification is sent to Infosec
4. Infosec review request and approves or rejects
5. Support case is updated
6. Notification is send to client
7. If approved, the client then chooses a time for the change to be pushed to network
8. Change push at the time nominated in step 3

This process will be expanded upon as needed.

Each change to a workspace is automatically tracked and versioned live as the admin makes the edits. The changes, however, do not get applied to endpoints to be enforced immediately. This is done through a separate process via the "Enforce Latest Policies" button in the Tetration GUI. The idea is that an admin can make changes, then run some analysis in TA to understand what the impact of the change would be should it be implemented. Unintended negative impacts can then be handled by further edits to the policy. Once the admin is happy, they hit the enforce latest policies button at which point the changes are pushed out to the agents on the endpoints and the updated policy is

applied.

As Cisco IT pushes network security policy into the end points via the Tetration enforcement agent, it is important to monitor and report on the status of those agents. If a hacker can get access to the operating system of a host, it's feasible that he/she could disable the agent and circumvent the policy that should be enforced. Monitoring and reporting of the status of the agents mitigates this risk and is an infosec requirement.

Cisco IT is incrementally building out these monitoring, reporting and remediation capabilities:

- TA agent status report
- Alerts for TA agents considered 'critical'
- Auto-notification to owner of server
- TA agent status dashboard
- Auto-quarantine of server
- Auto-remediation of server

Tetration Agent Status Report

Cisco IT generates a report that aggregates details the Tetration agents that are non-compliant to their expected status. Non-compliance can mean that the agent is offline or that the policy rules set on the host, does not match those on the cluster

- An agent is considered offline if it has not had communication to the TA cluster for longer than 15 minutes
- If the server itself is offline (e.g.: powered off), then it is not considered offline from a TA agent perspective
- An agent is considered non-compliant if the policy rule set configured on the TA cluster does not match those configured on the end host by the agent

The report evaluates certain attributes regarding the level of severity.

- Network Security Zone - DMZ, buffer, internal
- Length of time agent has been offline

The report categories any non-compliant agents into critical, urgent, standard based on the table below:

	DMZ	Buffer	Internal
Between 15 and 30 mins	Standard	Standard	None
Between 30 and 60 mins	Urgent	Standard	None
Between 1 and 4 hours	Critical	Urgent	Standard
Between 4 and 24 hours	Critical	Critical	Standard
Between 1 and 5 days	Critical	Critical	Urgent
Over 5 days	Critical	Critical	Urgent

The report is emailed to the appropriate event resolution owner(s).

Any non-compliant Tetration agent deemed to be critical generates an alert in ServiceNow for the data center network operations team. The owner of the server is emailed a notification for any offline Tetration agent. The email notification includes a link to documentation on suggested remediation steps and escalation points. If a server can be mapped to a particular application, then the application owner receives a copy of the email.

Auto-Quarantine Under Consideration

Cisco IT is considering deploying auto-quarantine. In some cases where a Tetration agent is non-compliant, the server can be placed into quarantine.

The criteria for determining if a host should be auto quarantined is a combination of:

- Network Security Zone
- Length of time agent has been offline

This quarantine provides enough access for a system admin to remedy the fault.

Best Practices and Lessons Learned

Start off focused on application dependency mapping: . Cisco IT found that

Tetration machine learning effectively automates application dependency mapping. Tetration can export ACI contract specifications in various formats, including XMP, JSON, and YAML. The Tetration generated contracts specify how data flows are allowed between EPGs. Cisco IT incorporates the contract specifications into its standard YAML library which is then posted to ACI.

Start off focused on the basics: add new features as you go, and test/certify new features and code prior to production deployment. Use lab environments for testing prior to production rollout, and check release notes for any important changes. Create a certification process with standard must have capabilities and verification, and document/track issues found. Use border leaf even / border leaf odd maintenance groups.

Build with automation in mind: create standard and reusable constructs, and document naming conventions for various objects to make readability and troubleshooting easier. Scripting skills will help you on your journey.

Schedule secure configuration backups/archives daily.

Security: Cisco IT found that Tetration scopes and RBAC support enabled them to build a layered more security as well as agile security posture for its data centers. As for automation of enforcement, Cisco IT is still evaluating that capability for future consideration.