cisco Secure

Cisco Secure Network Analytics Customer Test Drive

Learn how to turn your network into a sensor and enforcer using behavioral analytics and machine learning

Updated Jun 2021

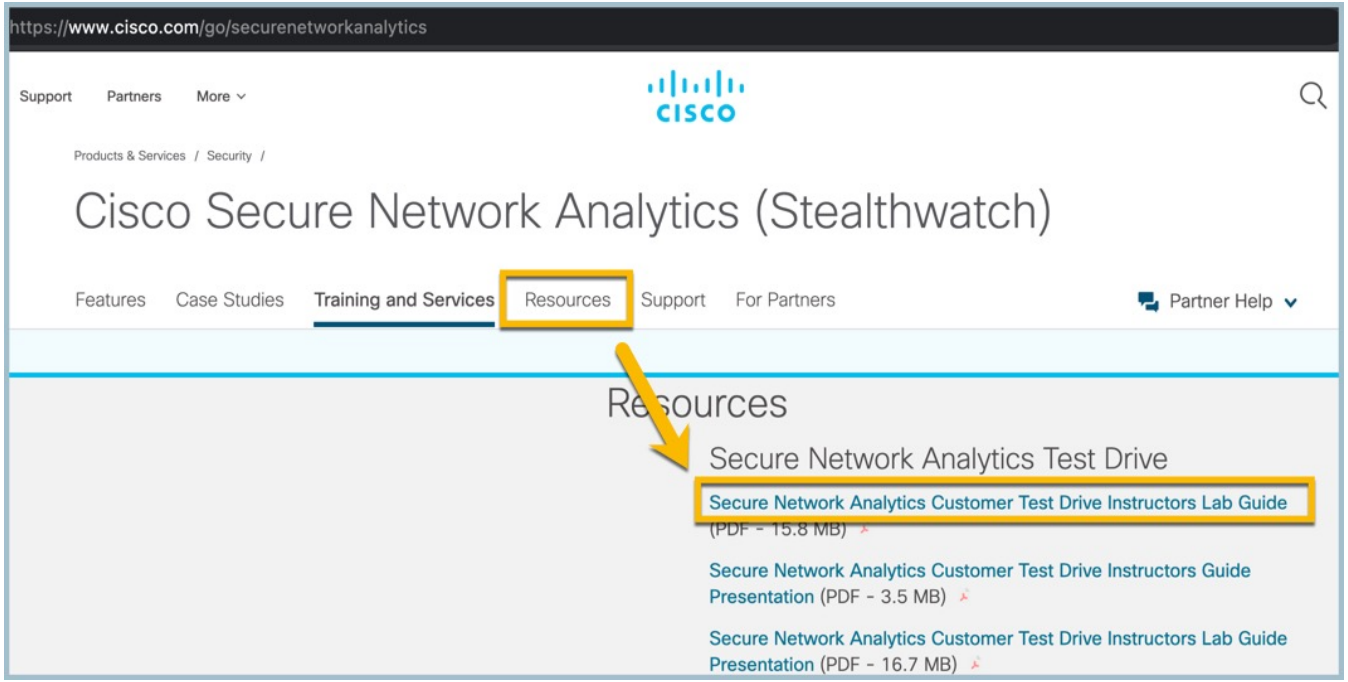
Welcome

Hands on labs

1. Overview and Lab Setup
2. Breach Detection Labs
3. Insider & Advanced Threat Detection Labs
4. High Risk Application Detection Labs
5. Policy Violation Labs
6. Encrypted Traffic Analytics
7. Public Cloud Monitoring

Lab Guide Download

https://www.cisco.com/go/securenetworkanalytics



cisco Secure

Overview and Lab Setup

NOTE: There are additional labs in the appendix that are optional. This include how to configure netflow, ETA, and SIEM integration.

Disclaimer

This lab should be running for at least 1 hour before performing exercises. For best results let the lab run for at least 24 hours before starting exercises.

dCloud is a powerful lab environment for education purposes. There are often thousands of different types of labs running simultaneously. To allow for more labs to run within the dCloud datacenters, resources are shared across labs which could cause slower than normal response times during heavy usage.

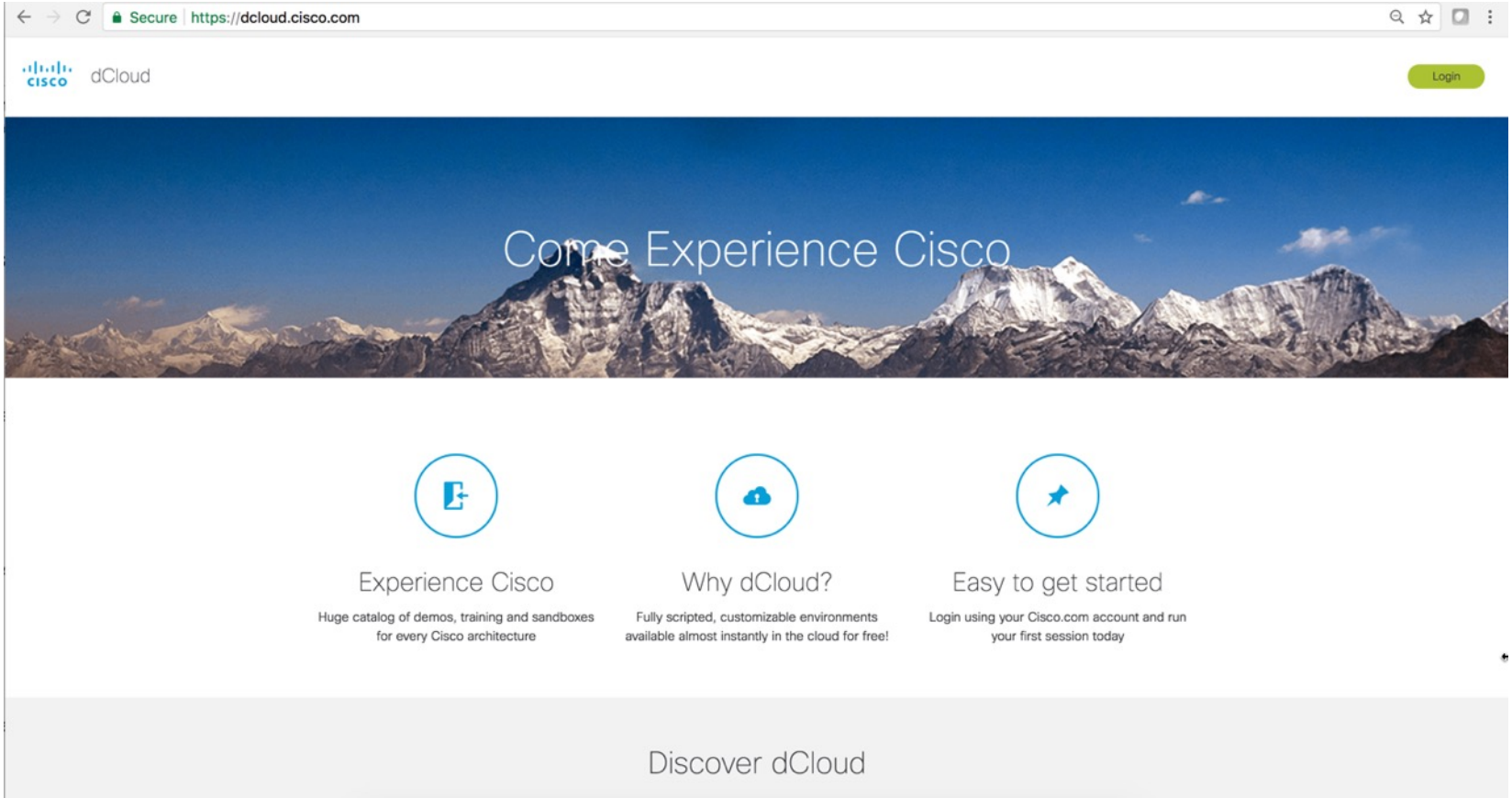
Secure Network Analytics requires reserved resources of RAM and CPU in production deployments. Within these labs we do not have the RAM and CPU reserved. Please note: any slowness in queries or detection could be caused because of this so allow extra time for results.

It may take:

- Flow records 1-2 minutes after generating traffic to appear in Secure Network Analytics
- Events will appear 5-30 minutes after traffic is generated.

Cisco’s dCloud

Prove out use cases in a fully configured environment

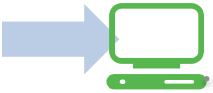


dCloud Lab Environment

Breach a fully setup data center with live attack traffic that you generate

Lab Network Highlights

You will connect to the Remote Workstation and VPN into the Datacenter



Remote VPN
198.18.1.36

Internet

Public Cloud Workloads

amazon web services

Web Mid DB

FW-198.19.10.1

CSR-198.19.20.1

Datacenter02

Remote Desktop Server exposed to the Internet:

198.19.30.36

You will login with stolen credentials

Datacenter02:
198.19.10.0/24
198.19.20.0/24
198.19.30.0/24
198.18.1.0/24

WAN01-172.16.16.3

FW-172.16.16.2

CORE-172.16.16.1

Users Segment
10.201.3.0/24

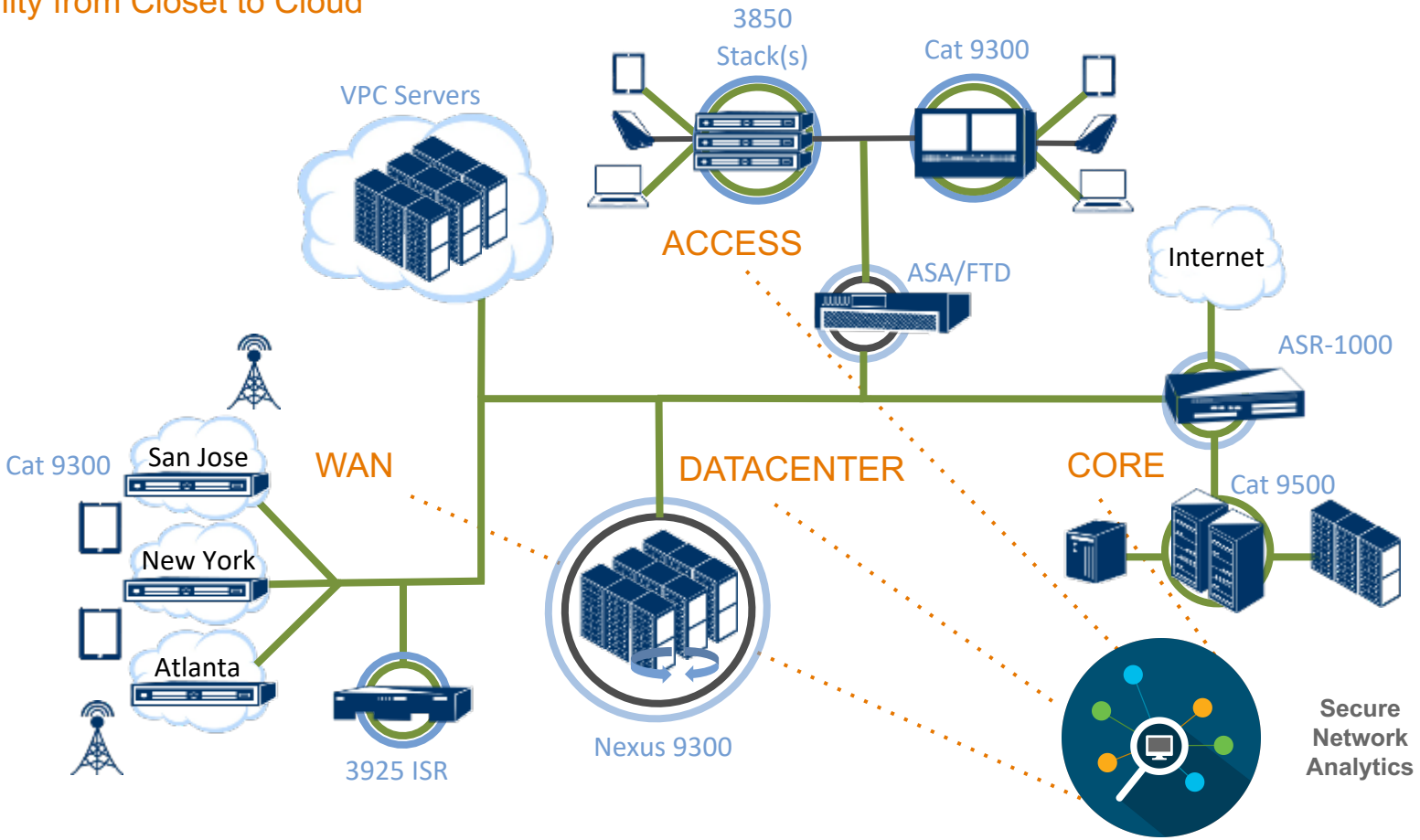
Datacenter01:
10.201.0.0/24
209.182.184.0/24

Replica of real customer network

cisco

The Network is Your Sensor

Visibility from Closet to Cloud



Overview Lab

- Getting Started
- Validating Your Wkst1 – ipconfig
- Validating Your Wkst1 – Install Tor Browser
- Validating Your Wkst1 – netstat
- Validating Your Wkst1 – Flow Search

Summary

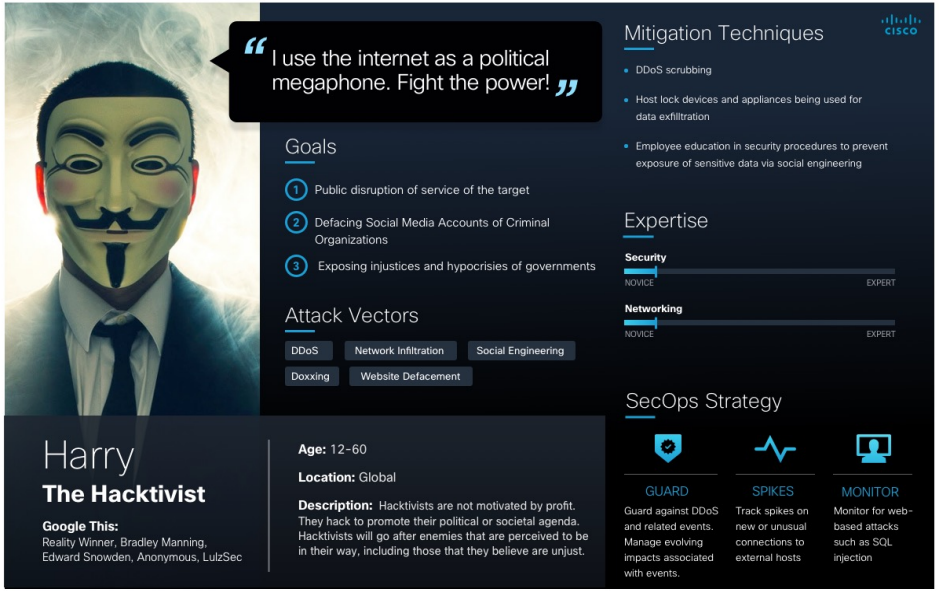
Within this lab you learned:

- Became familiar with WKST1 that you connected to in the datacenter
- Learned that all network conversations are accounted for from this machine through NetFlow collection
- Learned how to run a basic Flow Search in Secure Network Analytics to see all https flow between your Wkst1and the Internet (Outside Hosts)

☑ End of Lab: Please pause here.

Stop here (p. 20)

Breach Detection Labs



1. Remote Access Breach using stolen credentials (with Recon)
2. Monitoring Trusted 3rd Party and VPN Access with ISE ANC
3. Historical traffic analysis to identify threats to Suspect Countries

Watch video
https://youtu.be/UzvPP6_LRHc

Breach Detection

Can it really be this easy for the attacker?

TV5Monde's disregard of security exposes passwords on live television

After suffering a hack that took the TV station offline, live interview with reporter displays usernames and passwords written on sticky notes

▲ TV5Monde's lax approach to security, writing usernames and passwords on sticky notes on walls, may have contributed to its hacking. Photograph: Yoan Valat/EPA

Reference: https://www.theguardian.com/technology/2015/apr/10/tv5monde-isis-security-exposed-passwords-live-television

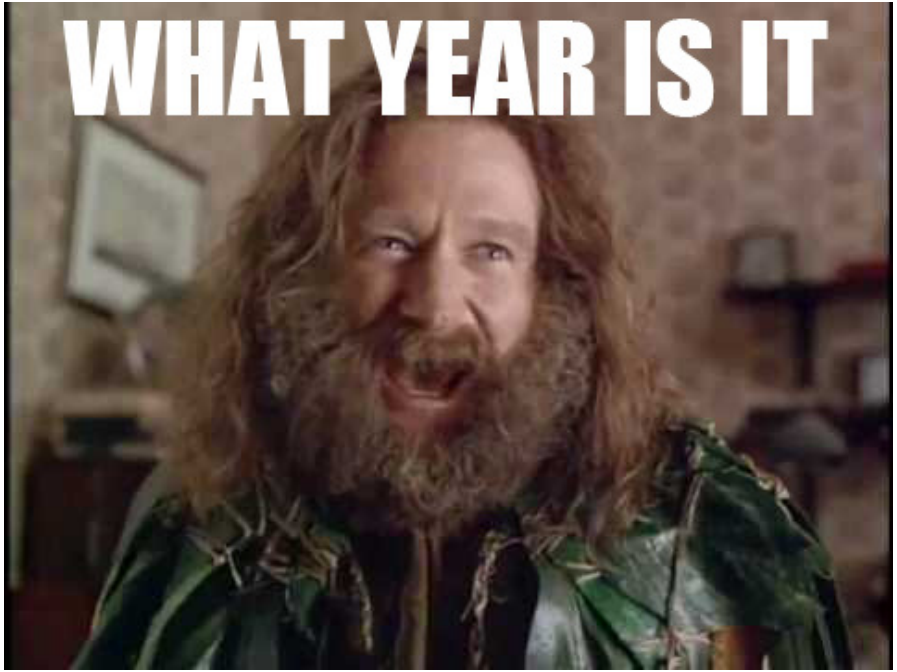
Stolen credentials?

“81% of hacking-related breaches leveraged either stolen and/or weak passwords.”

Verizon Data Breach Investigation Report

Check your own email address for compromise here:

https://haveibeenpwned.com/



Summary

Within this lab you learned:

- The importance of accounting for all traffic to and from the Internet
- How to perform network retrospection to suspect countries
- How to detect threats hidden within trusted network connections
- How to filter on flow connections over long periods of time to help identity possible command and control traffic
- How to filter on data movement over long periods of time to help identify possible data loss
- Understanding how you can learn from having complete visibility and accounting to make better decisions in segmenting traffic to help prevent threats.

Watch supporting lab videos
Breach Detection
Lab 1: https://cs.co/SWTestDrive-Lab1
Lab 2: https://cs.co/SWTestDrive-Lab2
Lab 3: https://cs.co/SWTestDrive-Lab3

☑ End of Lab: Please pause here.

Stop here (p. 54)

Insider & Advanced Threat Detection

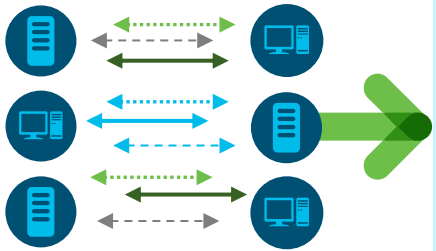
The attacker does their homework

Watch video
https://youtu.be/4gR562GW7TI

Behavioral and Anomaly Detection Model

Behavioral Algorithms are Applied to Build “Security Events”

Collect and Analyze Flows



Flows

Security Observations

Addr_Scan
..
Bad_Flag_ACK**
Beaconing Host
Bot Infected Host - Successful
Brute Force Login
Fake Application
Flow_Denied
..
ICMP Flood
..
Max Flows Initiated
Max Flows Served
..
Suspect Data Hoarding
Suspect Data Loss
Suspect Long Flow
..
UDP Received

Alarm Category

- Concern
- Recon
- C&C
- Exploitation
- Data hoarding
- Exfiltration
- DDoS target

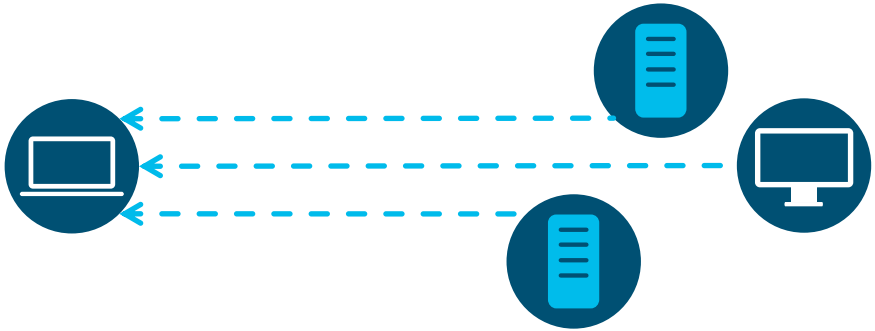
Response

- Alarm table
- Host snapshot
- Email
- Syslog / SIEM
- Mitigation

Example Algorithm: Data Hoarding

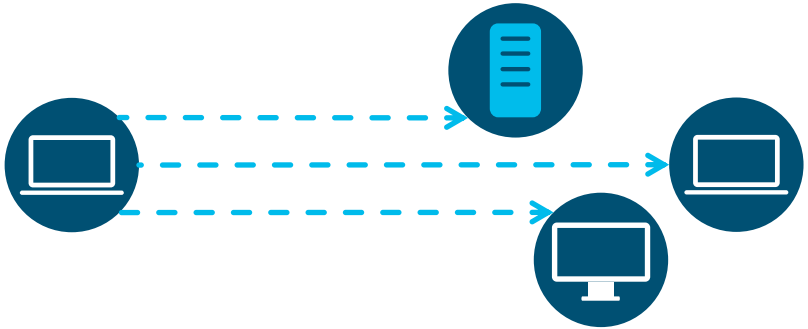
Suspect Data Hoarding

Unusually large amount of data inbound from other hosts



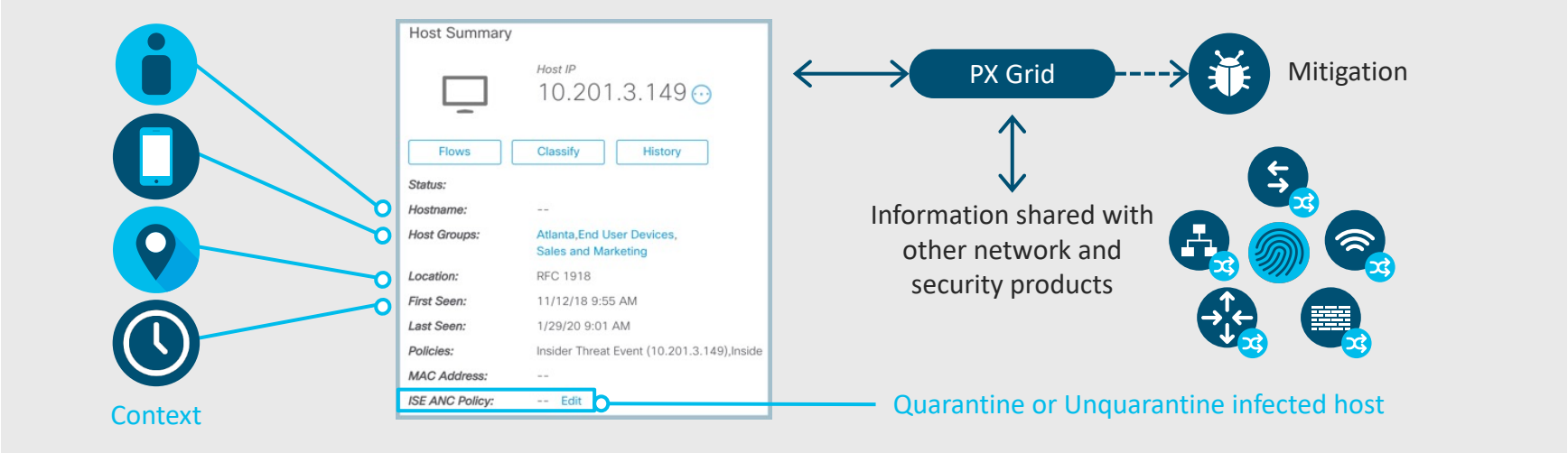
Target Data Hoarding

Unusually large amount of data **outbound from a host to multiple hosts**

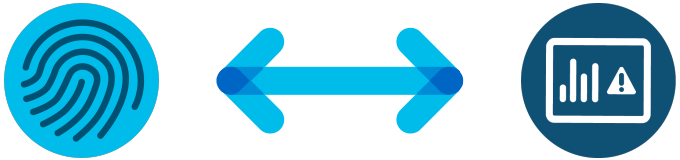


Rapid Threat Containment

Without any business disruption

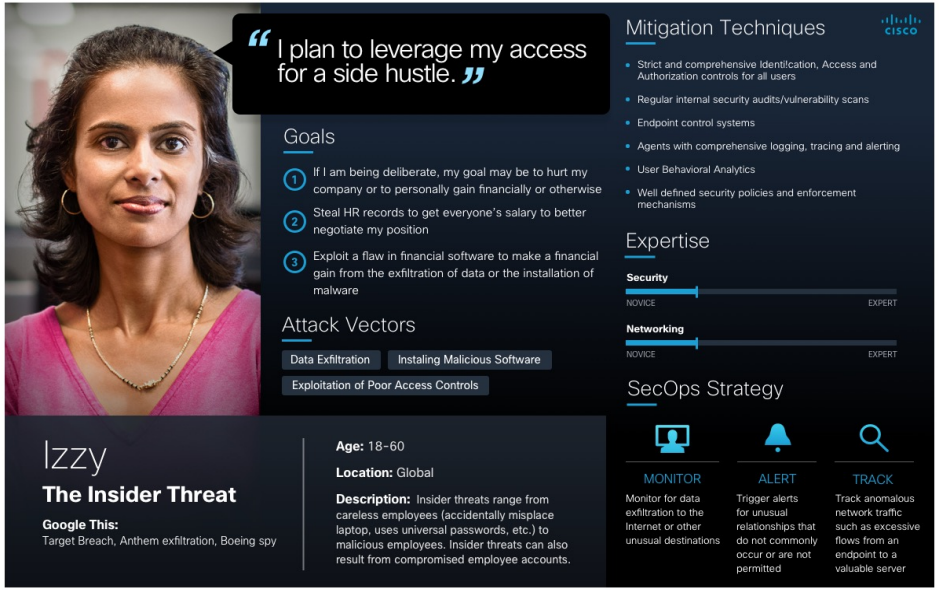


Cisco®
Identity Services Engine



Stealthwatch
Management Console

Insider & Advanced Threat Detection



Labs

4. Data Hoarding
5. Data Exfiltration

Summary

Within this lab you learned:

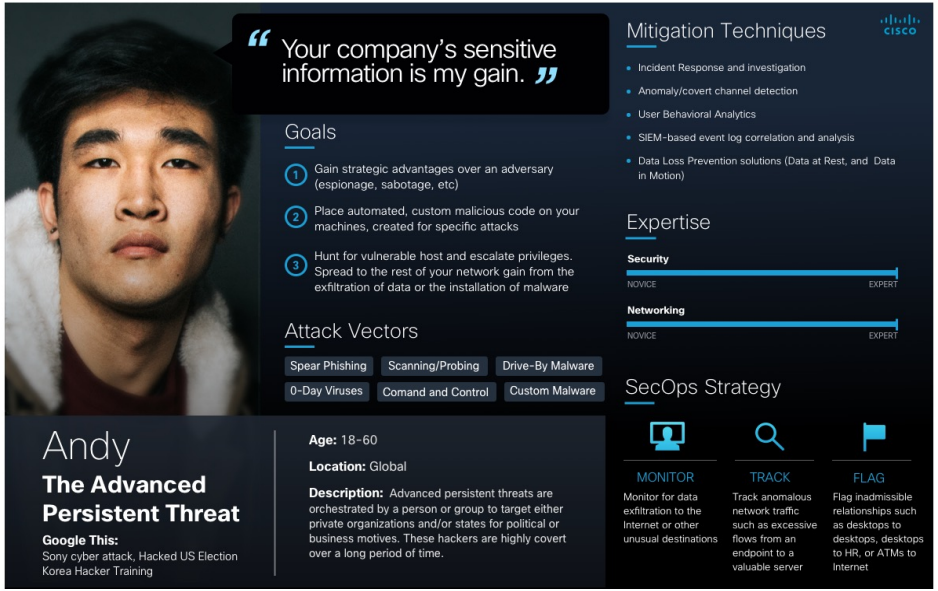
- How to trigger alarms for data hoarding activity.
- How to review the data hoarding alarms within Secure Network Analytics.
- How to trigger alarms for data exfiltration activity
- How to review Secure Network Analytics data exfiltration alarms

Watch supporting lab videos
Insider & Advanced Threat Detection
Lab 4: https://cs.co/SWTestDrive-Lab4
Lab 5: https://cs.co/SWTestDrive-Lab5

☑ End of Lab: Please pause here.

Stop here (p. 68)

High Risk Application Detection



Labs

6. Telnet Violation
7. SMB Traffic to Internet

Summary

Within this lab you learned:

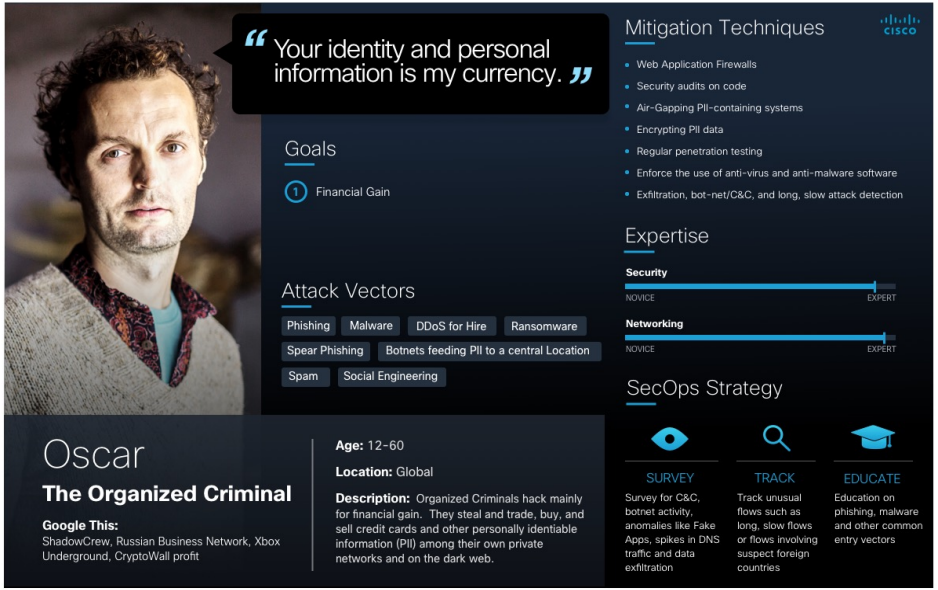
- How to create a Custom Security Event for Telnet communications
- How to generate telnet traffic from the network
- How to review the Network Security dashboard for Custom Security Alarms
- How to simulate SMB traffic using nmap.
- How to review the Network Security dashboard for Top Alarming Hosts

Watch supporting lab videos
High Risk Applications
Lab 6: https://cs.co/SWTestDrive-Lab6
Lab 7: https://cs.co/SWTestDrive-Lab7

☑ End of Lab: Please pause here.

Stop here (p. 84)

Policy Violations



Labs

8. Network segmentation violations
9. Rogue Server Detection

Summary

Within this lab you learned:

- How host groups can automatically be updated. There is a Host Group Automation service that may be purchased to simplify synching your IPAM with the SMC host group tree.
- How to create a custom security event
- How to generate traffic to a Custom Security Event
- How to investigate through the Host Group Report
- How to view added context within the Flow Table results
- How to create a custom security event to detect rogue DNS servers
- How to trigger and then investigate a rogue DNS server event

Watch supporting lab videos
Policy Violations
Lab 8: https://cs.co/SWTestDrive-Lab8
Lab 9: https://cs.co/SWTestDrive-Lab9

☑ End of Lab: Please pause here.

Stop here (p. 104)

Encrypted Traffic Analytics (ETA)

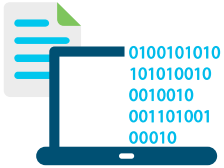
http://www.cisco.com/go/eta

Watch video

https://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-security/eta.html?socialshare=lightbox-acnhor

Encrypted Traffic Analytics (ETA)

Visibility and malware detection without decryption



Detect Malware in encrypted traffic

Is the payload within the TLS session malicious?

- End to end confidentiality
- Channel integrity during inspection
- Adapts with encryption standards

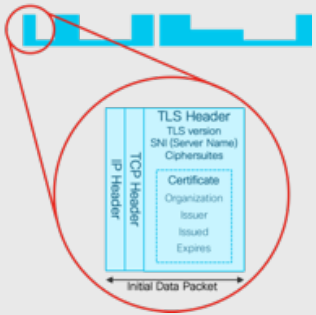
Verify cryptographic compliance

How much of my digital business uses strong encryption?

- Audit for TLS policy violations
- Passive detection of Ciphersuite vulnerabilities
- Continuous monitoring of network opacity

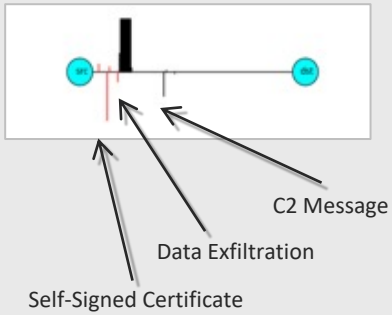
Data elements to analyze encrypted traffic

Initial data packet



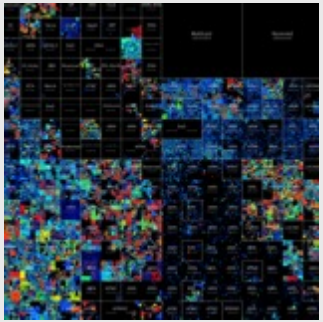
Make the most of unencrypted fields

Sequence of packet lengths and times



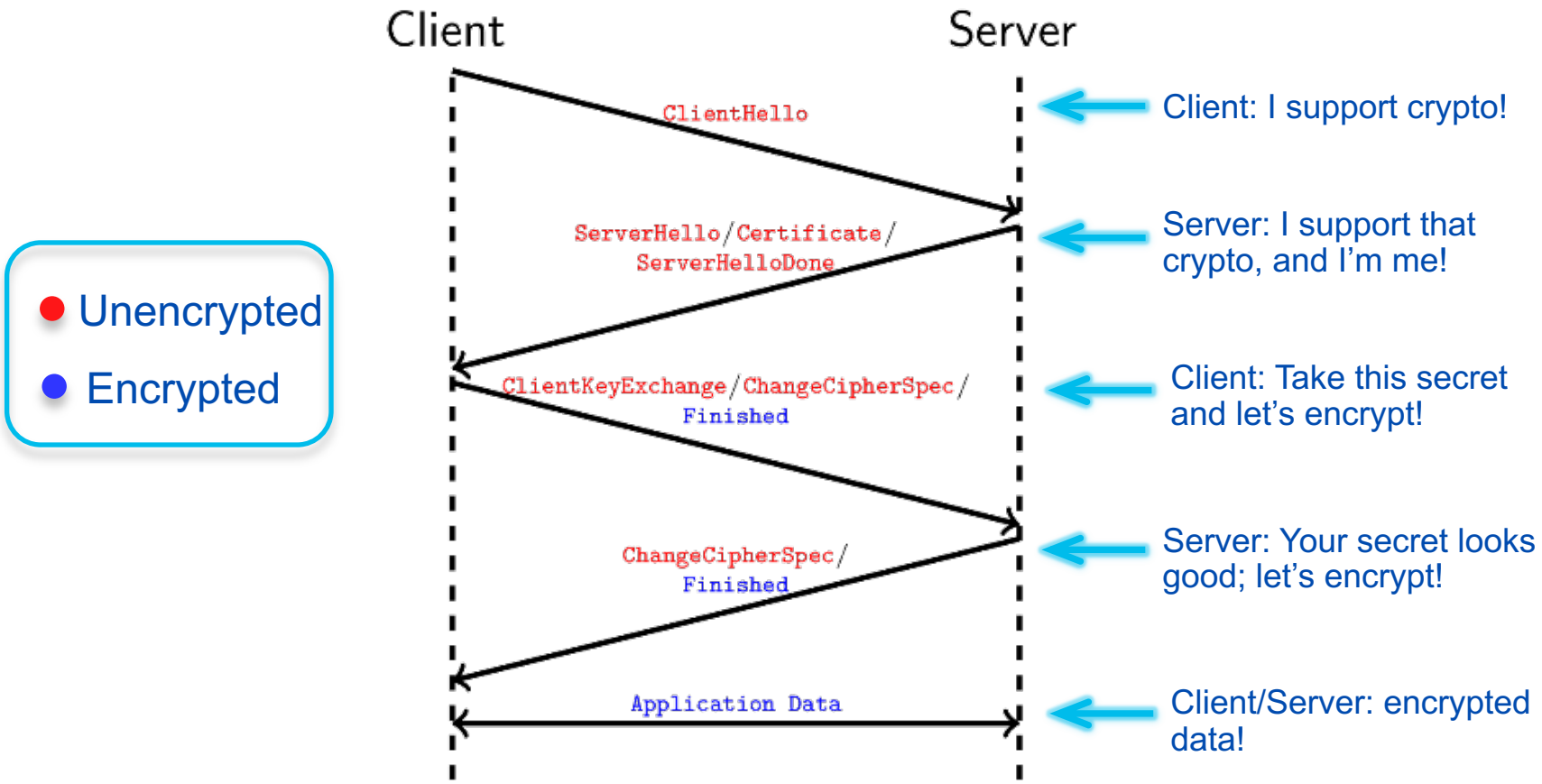
Identify the content type through the size and timing of packets

Global Risk Map



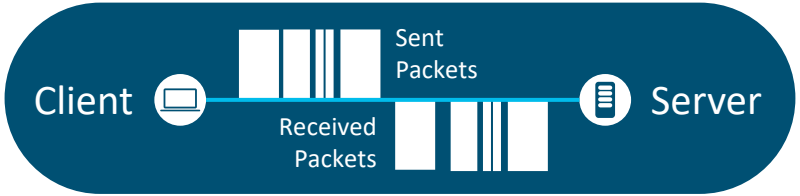
Know who's who of the Internet's dark side

Transport Layer Security (TLS) Handshake - IDP



Identifying malicious encrypted traffic

Model



Packet lengths, arrival times and durations tend to be inherently different for malware than benign traffic

Google Search Page Download

Initiate Command and Control

Exfiltration and Keylogging

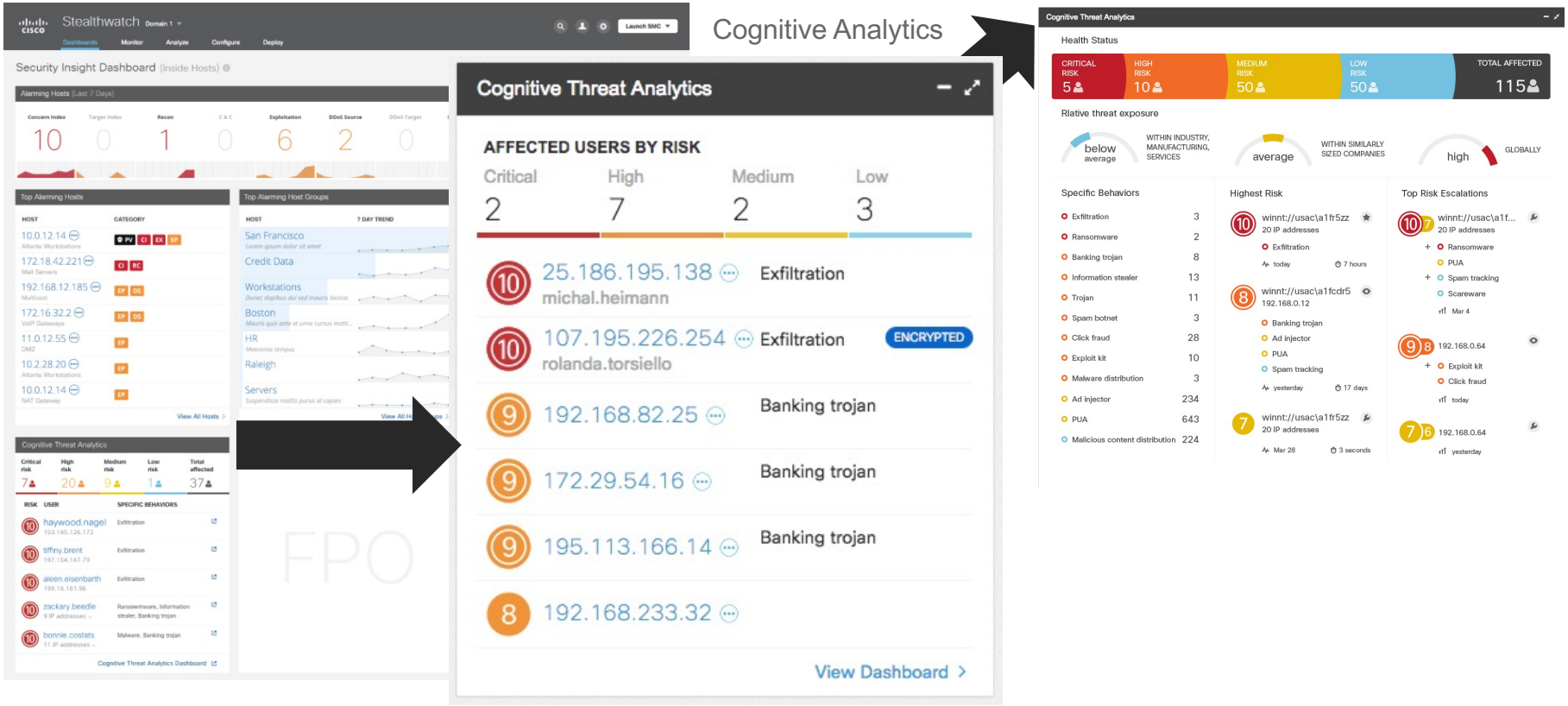
Encrypted Traffic Analytics Elements

Leveraged network	Faster investigation	Higher precision	Stronger Protection
Enhanced NetFlow from Cisco's newest switches and routers	Enhanced analytics and machine learning	Global-to-local knowledge correlation	Continuous Enterprise-wide compliance

Encrypted Traffic Analytics

Cognitive Analytics

Expanded CTA Dashboard View



Encryption Details on all Network Flows

Stealthwatch

Dashboards | Monitor | Analyze | Jobs | Configure

Desktop Client

Flow Search Results (236)

Edit Search | Last 12 Hours (Time Range) | 2,000 (Max Records)

Save Search | Save Results | Start New Search

Subject: Either (Orientation)

100% Complete | Delete Search

Connection: All (Flow Direction) | TLS 1.2 (Encryption TLS/SSL Version)

Manage Columns | Summary | Export

START	DURATION	SUBJECT IP A...	SUBJECT PO...	SUBJECT BYT...	APPLICATION	TOTAL BYTES	TLS/SSL VERSION	KEY EXCHANGE	AUTHENTICATION ALGORITHM	KEY LENGTH	ENCRYPTION MAC	PEER IP ADDR...	PEER PORT/P...	PEER B
Ex. 06/09/2	Ex. <=50min4(	Ex. 10.10.10.1	Ex. 57100/UDI	Ex. <=50M	Ex. "Corporate	Ex. <=50M	Ex. 1.0	Ex. ECDH	Ex. ECDSA	Ex. AES_256_	Ex. SHA384	Ex. 10.255.25	Ex. 2055/UDP	Ex. <=
Aug 28, 2018 9:37:22 AM (57min 47s ago)	4min 16s	.3.51	49233/TCP	49.28 K	HTTPS (unclassified)	1.77 M	TLS 1.2	ECDHE	ECDSA	AES_128_GCM/128	SHA256	.77.36	443/TCP	1.72 M
Aug 28, 2018 1:37:24 AM (8hr 57min 45s ago)	4min 14s	.3.51	49233/TCP	49.28 K	HTTPS (unclassified)	1.77 M	TLS 1.2	ECDHE	ECDSA	AES_128_GCM/128	SHA256	.77.36	443/TCP	1.72 M
Aug 28, 2018 12:37:22 AM (9hr 57min 47s	4min 15s	.3.51	49233/TCP	49.28 K	HTTPS (unclassified)	1.77 M	TLS 1.2	ECDHE	ECDSA	AES_128_GCM/128	SHA256	.77.36	443/TCP	1.72 M

Devices Supporting ETA Export

- **Compatible Cisco Switches:**
  - Cisco Catalyst® 9300 Series (starting with the Cisco IOS XE Software Release 16.6.1) and the 9400 Series (starting with the Cisco IOS XE Software Release 16.6.2)
- **Compatible Cisco Routers:**

  Cisco ASR 1001-X, ASR 1002-X, ASR 1001-HX, ASR 1002-HX, ASR1000 RP2, ASR1000 RP3, ASR1000 ESP-40, 4221 ISR, 4321 ISR, 4331 ISR, 4351 ISR, 4431 ISR, 4451-X ISR, and ISR 1000 series routers, Cisco Integrated Services Virtual Router (ISRv), including the 5000 Enterprise Network Compute System, and Cisco Cloud Services Router (CSR) 1000V (starting with the Cisco IOS XE Software Release 16.6.2)
- **Wireless controllers:** Cisco Catalyst 9800 Series (starting with Cisco IOS XE Software Release 16.10.1)

Stealthwatch Flow Sensor

Installed on a mirroring port or network tap to generate telemetry based on the observed traffic. Available as hardware or virtual appliances (starting with Stealthwatch Software Release 7.1)

Encrypted Traffic Analytics (ETA)

http://www.cisco.com/go/eta

Labs

10. Cryto Audit Lab

Student should review:
https://cognitive.cisco.com

(this is bookmarked in Chrome on Wkst1)

While the instructor demos ETA malware detection

Summary

Within this lab you learned:

- How to enable Encrypted Traffic Analytics
- How to verify Encrypted Traffic Analytics
- How to use the Crypto Audit Report to detect policy violations
- How to detect malware within encrypted traffic

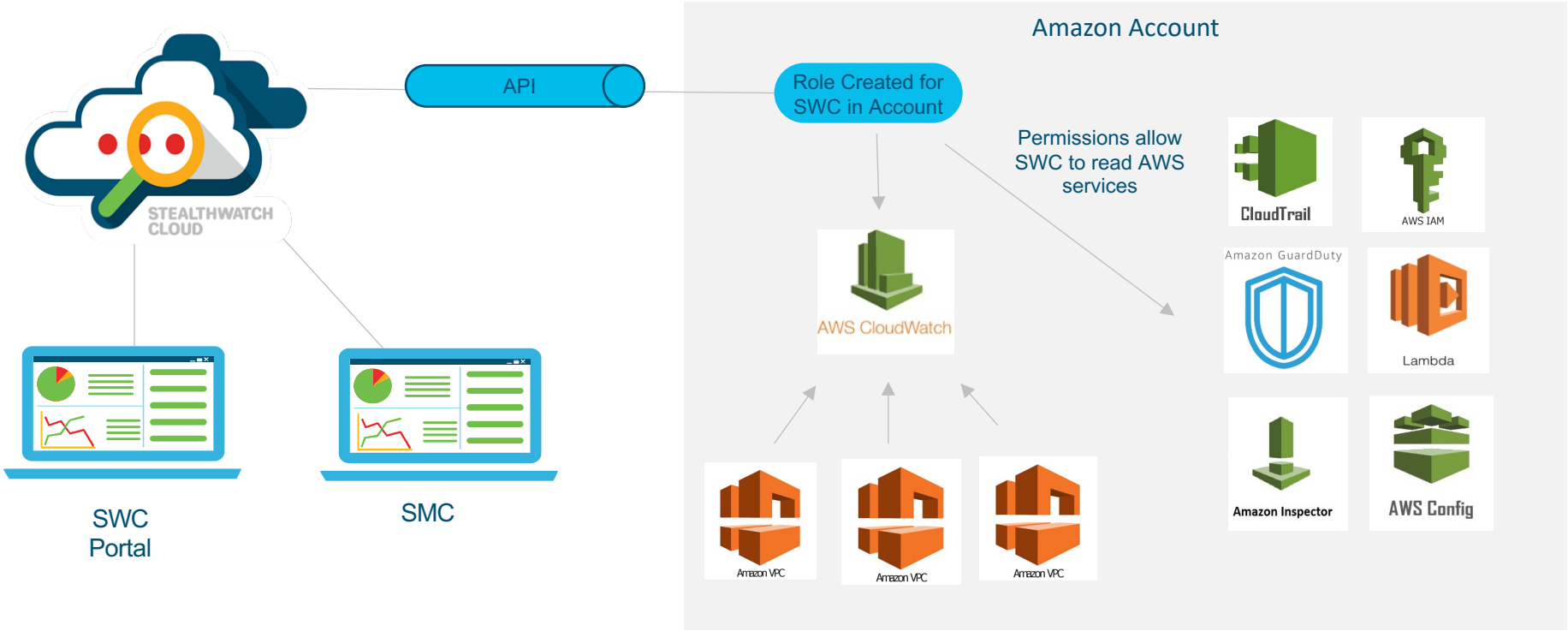
Watch supporting lab videos
Policy Violations
Lab 10: https://cs.co/SWTestDrive-Lab10
Lab 10: http://cs.co/SWTestDrive-Lab10-Crypto-Audit

☑ End of Lab: Please pause here.

Stop here (p. 118)

Public Cloud Monitoring

Amazon Web Services Deployment



What is a AWS VPC flow log?

Field	Description
version	The VPC flow logs version.
account-id	The AWS account ID for the flow log.
interface-id	The ID of the network interface for which the log stream applies.
srcaddr	The source IPv4 or IPv6 address. The IPv4 address of the network interface is always its private IPv4 address.
dstaddr	The destination IPv4 or IPv6 address. The IPv4 address of the network interface is always its private IPv4 address.
srcport	The source port of the traffic.
dstport	The destination port of the traffic.
protocol	The IANA protocol number of the traffic. For more information, go to Assigned Internet Protocol Numbers.
packets	The number of packets transferred during the capture window.
bytes	The number of bytes transferred during the capture window.
start	The time, in Unix seconds, of the start of the capture window.
end	The time, in Unix seconds, of the end of the capture window.
action	The action associated with the traffic: • `ACCEPT`: The recorded traffic was permitted by the security groups or network ACLs. • `REJECT`: The recorded traffic was not permitted by the security groups or network ACLs.
log-status	The logging status of the flow log: • `OK`: Data is logging normally to CloudWatch Logs. • `NODATA`: There was no network traffic to or from the network interface during the capture window. • `SKIPDATA`: Some flow log records were skipped during the capture window. This may be because of an internal capacity constraint, or an internal error.

	Time (UTC +00:00)	Message
	2019-06-09	
▾	21:37:47	2 299015533822 eni-0bd97f10b54af32da 10.0.0.241 178.137.18.211 15000 41598 6 1 40 1560116267 1560116295 ACCEPT OK
	2 299015533822 eni-0bd97f10b54af32da 10.0.0.241 178.137.18.211 15000 41598 6 1 40 1560116267 1560116295 ACCEPT OK	
▾	21:37:47	2 299015533822 eni-0bd97f10b54af32da 185.244.25.131 10.0.0.241 0 0 1 1 68 1560116267 1560116295 ACCEPT OK
	2 299015533822 eni-0bd97f10b54af32da 185.244.25.131 10.0.0.241 0 0 1 1 68 1560116267 1560116295 ACCEPT OK	

Lots of resources can generate flow logs


Amazon EC2


AWS Lambda


NAT gateway


Amazon Redshift


Amazon RDS

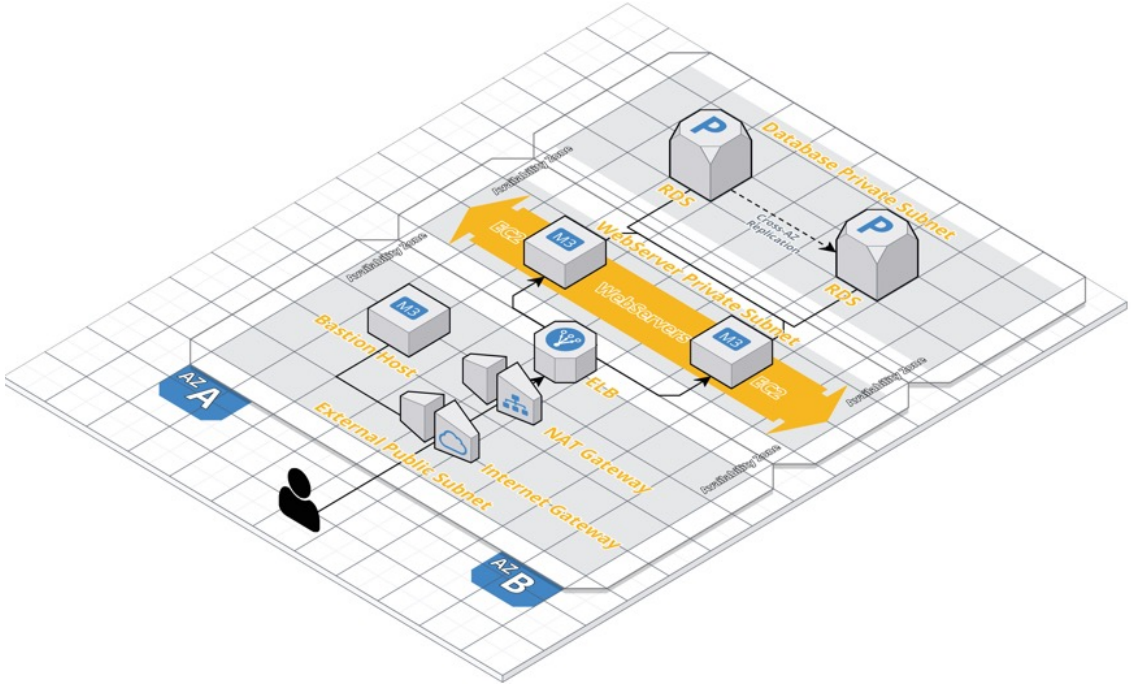

Amazon ElastiCache


AWS Transit Gateway


Elastic Load Balancing


Amazon VPC

Demo Setup



- Pair of RDS Database servers
- Pair of Web Servers
- Elastic Load Balance in front of the web servers
- Nat Gateway for egress traffic
- Bastion Host to get into the network remotely
- Separate Availability Zones

Secure Cloud Analytics Exercises

(details in test guide)

View cloud dashboard via the SMC

Investigate alarms in Secure Cloud Analytics

Use Stealthwatch cloud to view the AWS environment (users, network, roles, etc.)

Summary

Within this lab you learned:

- how to monitor and protect cloud hosted infrastructure using Stealthwatch cloud.

Watch supporting lab videos
Public Cloud Monitoring
Lab 11: https://cs.co/SWTestDrive-Lab11

☑ End of Lab: Please pause here.

Stop here (p. 143)

Services for Secure Network & Cloud Analytics

Accelerate value with Stealthwatch Services

Gain the most value from your Stealthwatch deployment with the proactive and ongoing support you need

Advanced Services

Optimize Stealthwatch deployments to meet business requirements, increase productivity, and reduce risk

Educational Services

Offer training and customer enablement to help customers improve their security posture and respond to evolving threats

Support Services

Provide proactive and reactive engagement along with ongoing customer management

Install and deploy Stealthwatch with confidence

Deployment Service

The Deployment Service for Stealthwatch enables network and security teams to closely align Stealthwatch with your overall security strategy and provides initial configuration, tuning and report configuration for maximum performance.

Key benefits

- **Increase return on investment** with error-free deployment
- **Reduce time to value and attain a higher level of confidence** in the efficacy of Stealthwatch
- **Learn from highly skilled Cisco Stealthwatch experts** in a half-day knowledge-transfer sessions customized for your technical team

Install with support

Manage with ongoing, targeted support

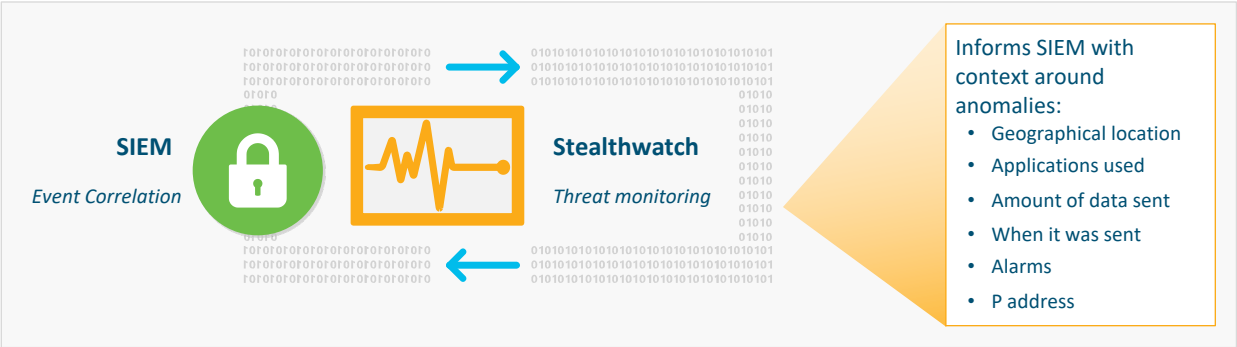
Seamlessly integrate with your SIEM

SIEM integration

The Stealthwatch Security Information Event Management (SIEM) Integration Service provides additional context around potential threats by combining alarm notification with flow data, so that customers can classify a threat and take appropriate action.

Key benefits

- **Streamline integration with security information event management (SIEM),** maximizing investment in your existing security infrastructure
- **Automatically pivot from SIEM to Stealthwatch to see top reports** such as top peers (IP destinations), top conversations, and top services
- **Leverage SIEM to gain deep network visibility into your network** with alarms from your entire system, displaying suspicious IP address activity



Utilize Host Group Automation services

Host group automation

The Stealthwatch Host Group Automation Service gives customers a logical means of categorizing network assets for improved visibility and control.

Key benefits

- **Automate host-group updates and management** to operate at maximum efficiency for alarm detection
- **Optimize Cisco Stealthwatch performance and reduce operational overhead** to lower operating costs while reducing errors and innocuous alerts
- **Enhance Stealthwatch system performance** by automatically managing your specific IP address base

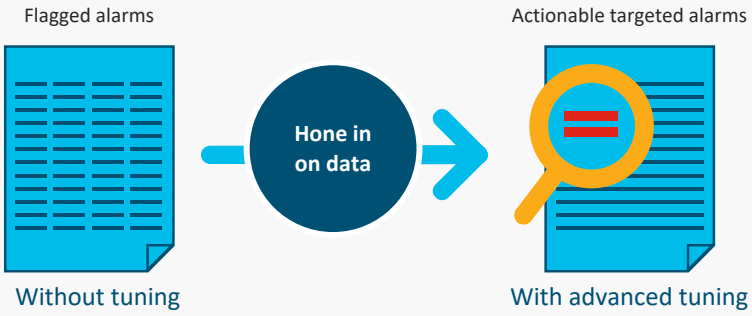
Operate efficiently with Health Check and Tuning Services

Health check and tuning services

The Stealthwatch Health Check and Tuning enables organizations to achieve increased operational efficiency and return on investment. Customers will benefit from high fidelity alarms, quicker response times and minimized corporate risk and control.

Key benefits

- **Tune your detection in advance of threats**
  through critical asset, location traffic mapping, achieving clear and actionable alarms
- **Customize alarms to your specific network environment**
  by looking at patterns in your network traffic, events and locations for performance
- **Understand the patterns that matter**
  by grouping critical assets and classifying known applications



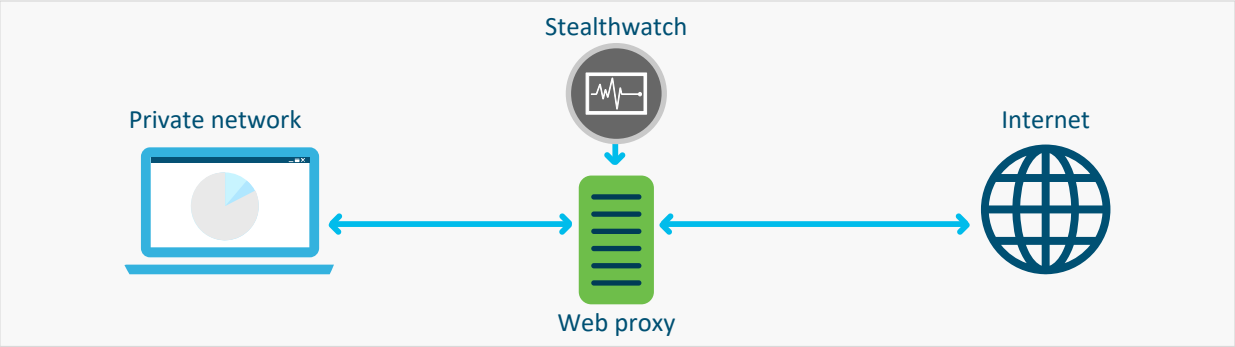
Integrate proxy records from web proxy server

Proxy Integration Service

The Security Stealthwatch Proxy Integration Service enables you to achieve end-to-end network visibility for improved threat detection and reduced corporate risk.

Key benefits

- **Stitch together external and internal sessions** to the internet from a specific user
- **Record activity over time of internet sessions** to historically investigate between 60-day to 120-day timeframes
- **Gain full end-to-end visibility** of command and control communications across the proxy server



Accelerate value with learning and education

Learning Services

Stealthwatch Learning Services enable your team to learn how to quickly detect and respond to their environment through a suite of learning resources, such as eLearning, technical and advanced courses, and customized trainings.

Key benefits

- **Learn Stealthwatch fundamentals and core concepts**
  with eLearning available to all customers and live monthly Webinars
- **Obtain a technical, hands-on learning experience**
  with private instructor-led trainings, adoption services, and use case workshops
- **Strengthen your role with structured curriculum**
  with users in success profiles such as administration, and network and security operations

Implement segmentation with complete confidence

Segmentation Implementation Services

Segmentation is a long term process. Our team is your advocate along the way, providing visibility and anticipating potential issues before they arise to ensure the successful implementation of segmentation to your network.

Key benefits

- **Ensure your segmentation strategy design will work for your company** through discovery, data collection, and end to end visibility
- **Keep your deployment on track** by anticipating, identifying and mitigating risks and issues
- **Maintain the long term health of your segmentation program** through compliance auditing, policy monitoring, and providing comprehensive visibility

Ensure your design will work for your company

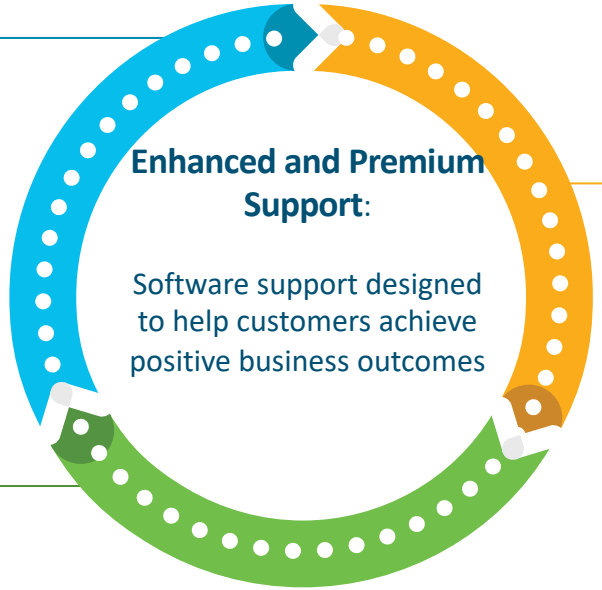
Keep your deployment on track

Maintain the long term health of your segmentation program

Cisco Stealthwatch Customer Maturity Model

Visibility

- NetFlow Configuration
- Context Collection
- Integrate Systems
- Professional Services
- Learning Services



Detection

- Initial Tuning
- Advanced Tuning
- Host Group Automation
- Professional Services
- Learning Services

Utilization

- Alarm Notification
- Incident Response Plan
- System Integration
- Professional Services
- Learning Services

Cisco Secure

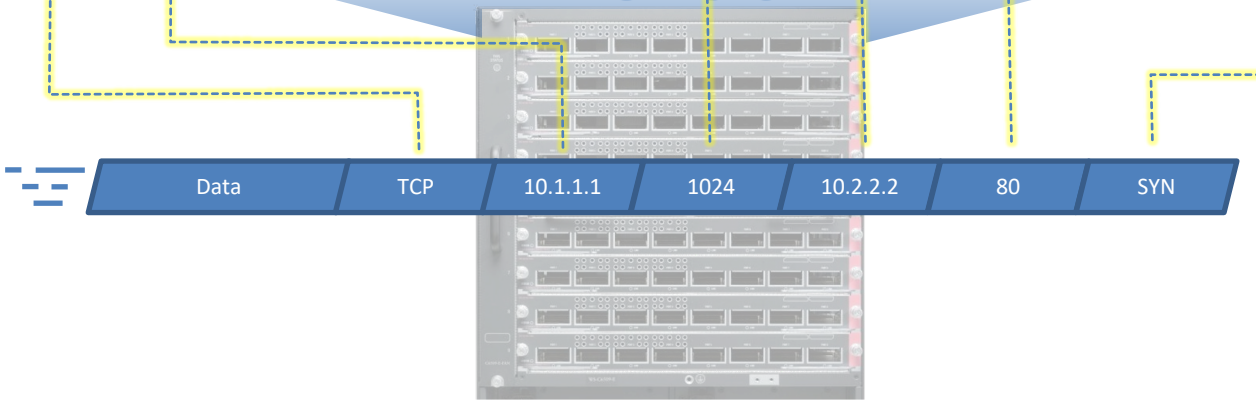
Netflow Overview and Lab

Create a New TCP Flow

Key Fields

Non-Key Fields

Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:06	1	195	Gi4/13	Gi2/1	S



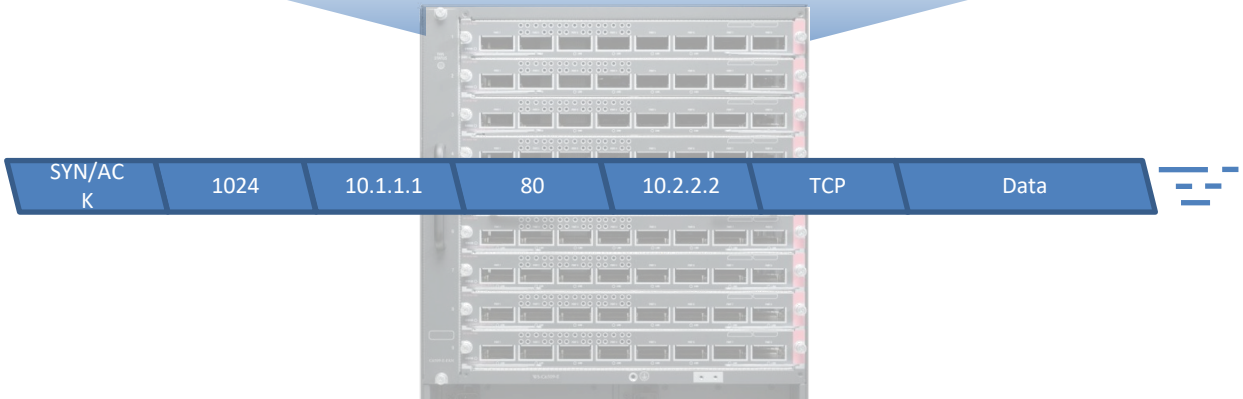
Lancope.

Create a New TCP Flow

Ingress and **Egress** ports are based on the interface on which the packets entered and left the router

Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:06	1	195	Gi4/13	Gi2/1	S
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.07	1	132	Gi2/1	Gi4/13	SA

NETFLOW CACHE

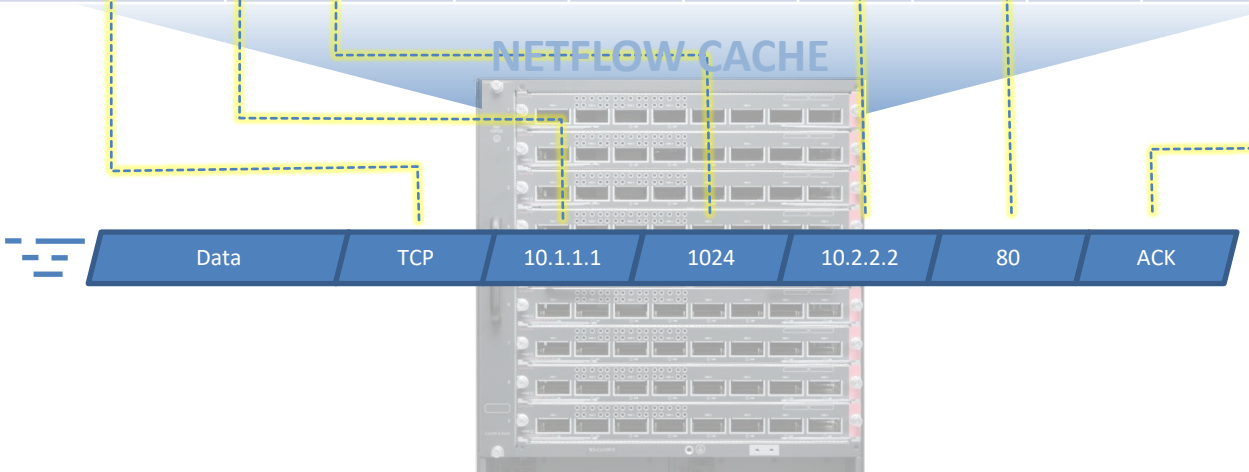


Lancope.

Update Existing TCP Flow

Packet and Byte counts are incremented accordingly. Last Seen is also updated.

Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:08	2	425	Gi4/13	Gi2/1	SA
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.07	1	132	Gi2/1	Gi4/13	SA

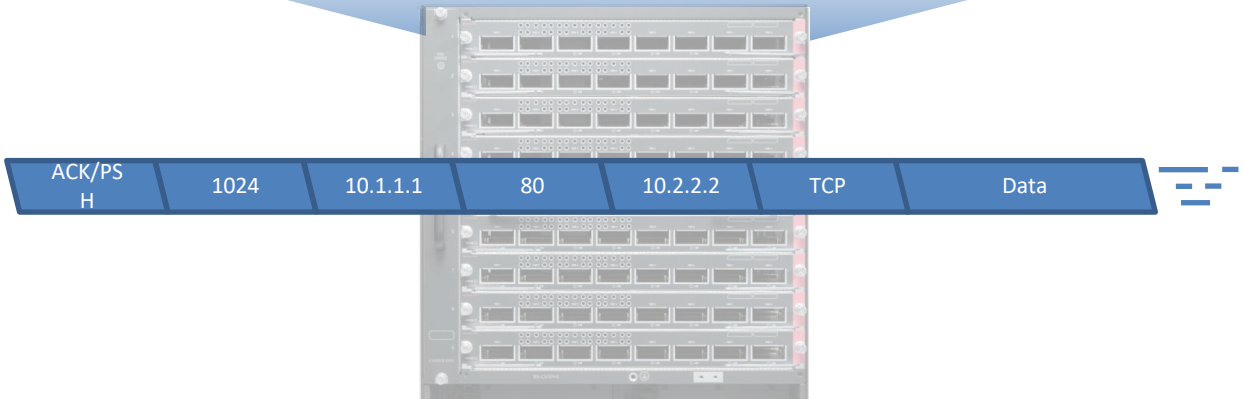


Lancope.

Update Existing TCP Flow

Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:08	2	425	Gi4/13	Gi2/1	SA
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.08	2	862	Gi2/1	Gi4/13	SAP

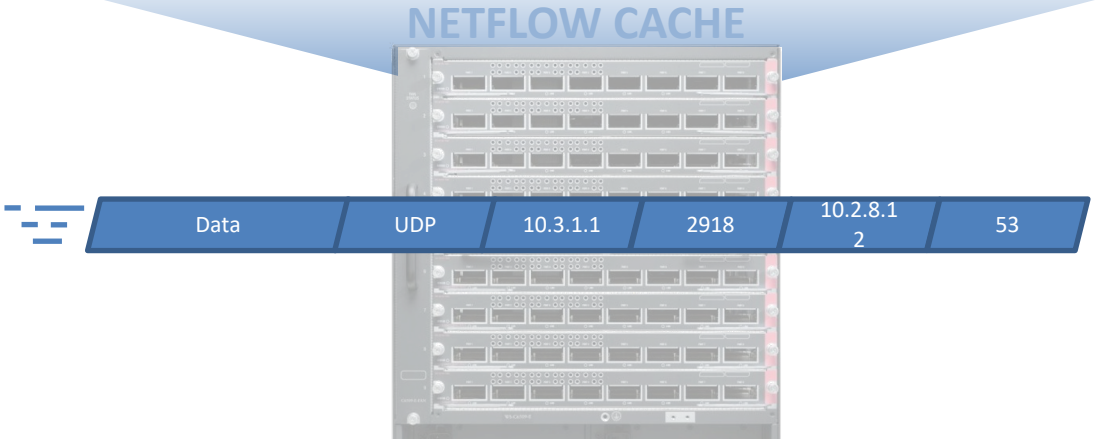
NETFLOW CACHE



Lancope.

Create New UDP Flow

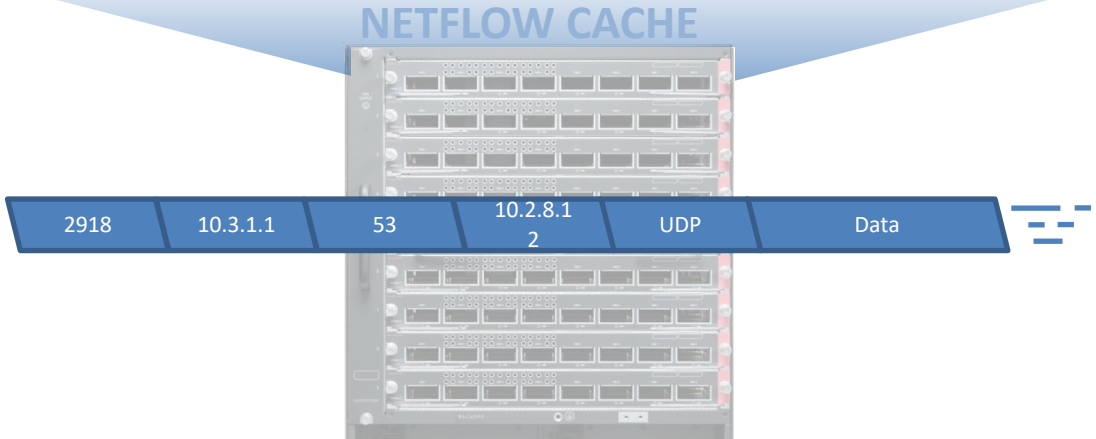
Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:08	2	425	Gi4/13	Gi2/1	SA
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.08	2	862	Gi2/1	Gi4/13	SAP
UDP	10.3.1.1	2918	10.2.8.12	53	23.14:11	23.14.11	1	176	Gi4/12	Gi2/1	-



Lancope.

Create New UDP Flow

Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:08	2	425	Gi4/13	Gi2/1	SA
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.08	2	862	Gi2/1	Gi4/13	SAP
UDP	10.3.1.1	2918	10.2.8.12	53	23.14:11	23.14.11	1	176	Gi4/12	Gi2/1	-
UDP	10.2.8.12	53	10.3.1.1	2918	23.14:11	23.14.11	1	212	Gi2/1	Gi4/12	-

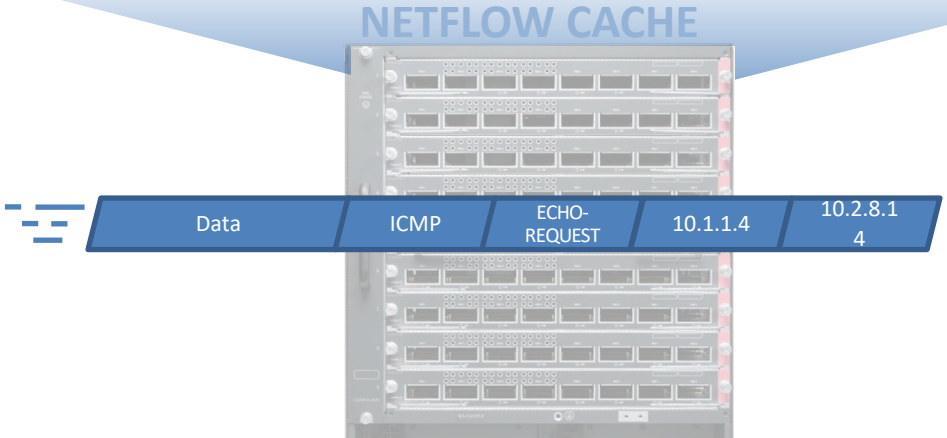


Lancope.

Create New UDP Flow

Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:08	2	425	Gi4/13	Gi2/1	SA
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.08	2	862	Gi2/1	Gi4/13	SAP
UDP	10.3.1.1	2918	10.2.8.12	53	23.14:11	23.14.11	1	176	Gi4/12	Gi2/1	-
UDP	10.2.8.12	53	10.3.1.1	2918	23.14:11	23.14.11	1	212	Gi2/1	Gi4/12	-
ICMP	10.1.1.4	-	10.2.8.14	ECHO-REQUEST	23.14.12	23.14.12	1	96	Gi4/19	Gi2/1	-

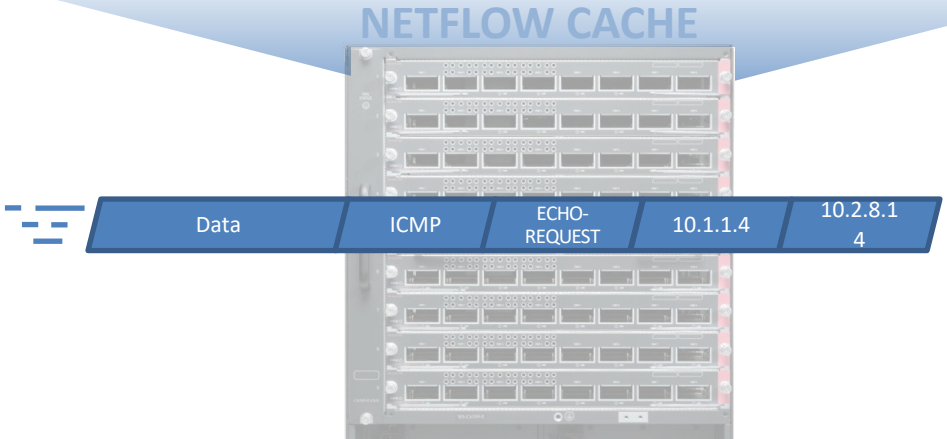
Most NetFlow caches do not offer ICMP type and code fields so the Destination Port column is overloaded with with ICMP information.



Lancope.

Update Existing ICMP Flow

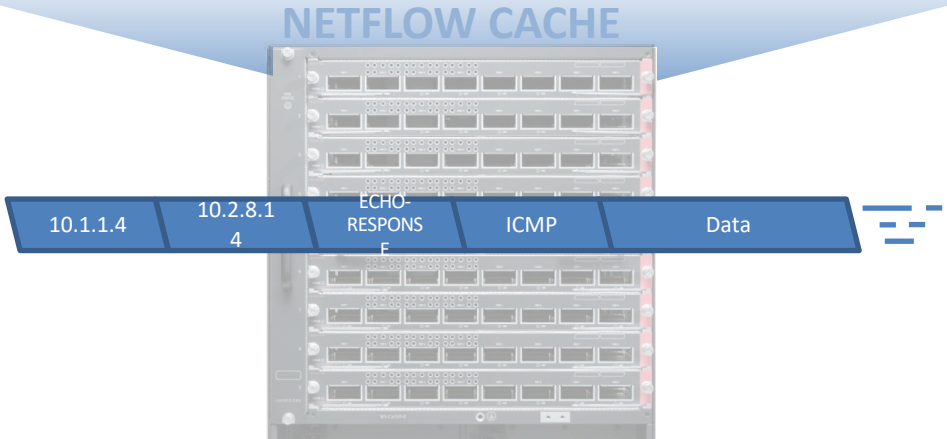
Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:08	2	425	Gi4/13	Gi2/1	SA
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.08	2	862	Gi2/1	Gi4/13	SAP
UDP	10.3.1.1	2918	10.2.8.12	53	23.14:11	23.14.11	1	176	Gi4/12	Gi2/1	-
UDP	10.2.8.12	53	10.3.1.1	2918	23.14:11	23.14.11	1	212	Gi2/1	Gi4/12	-
ICMP	10.1.1.4	-	10.2.8.14	ECHO-REQUEST	23.14.12	23.14.13	2	192	Gi4/19	Gi2/1	-



Lancope.

Create New ICMP Flow

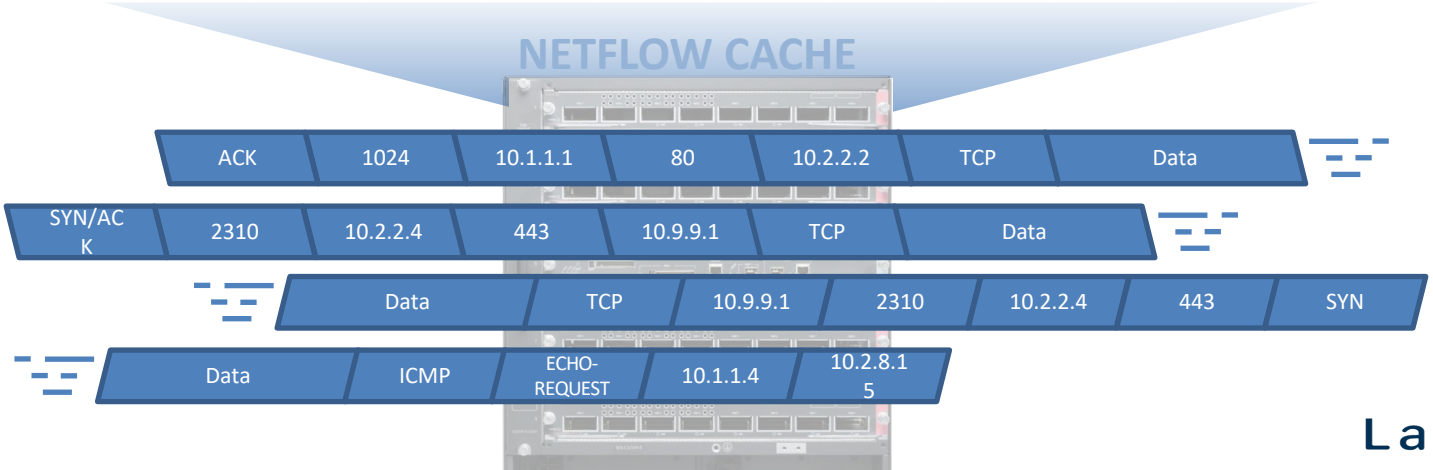
Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:08	2	425	Gi4/13	Gi2/1	SA
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.08	2	862	Gi2/1	Gi4/13	SAP
UDP	10.3.1.1	2918	10.2.8.12	53	23.14:11	23.14.11	1	176	Gi4/12	Gi2/1	-
UDP	10.2.8.12	53	10.3.1.1	2918	23.14:11	23.14.11	1	212	Gi2/1	Gi4/12	-
ICMP	10.1.1.4	-	10.2.8.14	ECHO-REQUEST	23.14.12	23.14.13	2	192	Gi4/19	Gi2/1	-
ICMP	10.2.8.14	-	10.1.1.4	ECHO-RESPONSE	23.14.13	23.14.13	1	92	Gi2/1	Gi4/19	-



Lancope.

Continued Operation

Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:08	2	425	Gi4/13	Gi2/1	SA
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.08	2	862	Gi2/1	Gi4/13	SAP
UDP	10.3.1.1	2918	10.2.8.12	53	23.14:11	23.14.11	1	176	Gi4/12	Gi2/1	-
UDP	10.2.8.12	53	10.3.1.1	2918	23.14:11	23.14.11	1	212	Gi2/1	Gi4/12	-
ICMP	10.1.1.4	-	10.2.8.14	ECHO-REQUEST	23.14.12	23.14.13	2	192	Gi4/19	Gi2/1	-
ICMP	10.2.8.14	-	10.1.1.4	ECHO-RESPONSE	23.14.13	23.14.13	1	92	Gi2/1	Gi4/19	-



Lancope.

Configuring NetFlow

1a. Configure the Exporter

```
Router(config)# flow exporter my-exporter
Router(config-flow-exporter)# destination 1.1.1.1
```

1b. Configure the Flow Record

```
Router(config)# flow record my-record
Router(config-flow-record)# match ipv4 destination address
Router(config-flow-record)# match ipv4 source address
Router(config-flow-record)# collect counter bytes
```

2. Configure the Flow Monitor

```
Router(config)# flow monitor my-monitor
Router(config-flow-monitor)# exporter my-exporter
Router(config-flow-monitor)# record my-record
```

3. Apply to an Interface

```
Router(config)# interface gi0/1
Router(config-if)# ip flow monitor my-monitor input
```

Creating Flows from Network Connections

{**Net●Flow**}

- *Network protocol developed by Cisco Systems for collecting IP traffic information.*

- **Based on 7 key fields (along with other data):**
  - 1. Source IP address
  - 2. Destination IP address
  - 3. Source port number
  - 4. Destination port number
  - 5. Layer 3 protocol type (ex. TCP, UDP)
  - 6. ToS (type of service) byte
  - 7. Input logical interface

If one field is different on an incoming packet, a new flow is created in the local flow cache.

NetFlow Records for Secure Network Analytics (minimum)

- Match ipv4 protocol
- Match ipv4 source address
- Match ipv4 destination address
- Match transport source-port
- Match transport destination-port
- Match interface input
- Match ipv4 tos
- Collect interface output
- Collect counter bytes
- Collect counter packets
- Collect timestamp system-uptime first
- Collect timestamp system-uptime last

Exporting Flow Records

#1 End of Flow

- RST or FIN packets seen on a flow will cause the flow record to be exported.

#2 Inactive Timeout

- Configures how long a flow can be inactive before it is expired from the cache
- Recommend 15 seconds (which is also the IOS default)
- All exporters should have similar inactive timeouts

#3 Active Timeout

- Configures longest amount of time a flow can stay in the cache regardless of activity
- Recommend 1 minute (Cisco default of 30 minutes is far too long)
- All exporters should have similar active timeouts

#4 Cache Full

- If the local Exporter Flow Cache fills up, the device will begin to export the oldest flows to make room for new flow tracking.

Last Seen – First Seen == Time Active

Protocol	Source IP	Source Port	Destination IP	Destination Port	First Seen	Last Seen	Packets	Bytes	Ingress Interface	Egress Interface	TCP Flags
TCP	10.1.1.1	1024	10.2.2.2	80	23:14:06	23:14:08	2	425	Gi4/13	Gi2/1	SA
TCP	10.2.2.2	80	10.1.1.1	1024	23.14:07	23.14.08	2	862	Gi2/1	Gi4/13	SAP
UDP	10.3.1.1	2918	10.2.8.12	53	23.14:11	23.14.11	1	176	Gi4/12	Gi2/1	-
UDP	10.2.8.12	53	10.3.1.1	2918	23.14:11	23.14.11	1	212	Gi2/1	Gi4/12	-
ICMP	10.1.1.4	-	10.2.8.14	ECHO-REQUEST	23.14.12	23.14.13	2	192	Gi4/19	Gi2/1	-

Git Basic Commands

$ git init	//Initialize Local Git Repository
$ git add <file>	//Add File(s) To Index
$ git status	//Check Status Of Working Tree
$ git commit	//Commit Changes In Index
$ git push	//Push To Remote Repository
$ git pull	//Pull Latest From Remote Repository
$ git clone	//Clone Repository Into A New Directory

Installing Git

- ✓ Linux (Debian)
  $ sudo apt-get install git
- ✓ Linux (Fedora)
  $sudo yum install git
- ✓ Mac
  http://git-scm.com/download/mac
- ✓ Window
  http://git-scm.com/download/win

CISCO Secure