



Cisco *live!*

6-9 March 2018 • Melbourne, Australia

It's all about Securing the Endpoint!

Ned Zaldivar, Security Architect

BRKSEC-2051

Cisco Spark

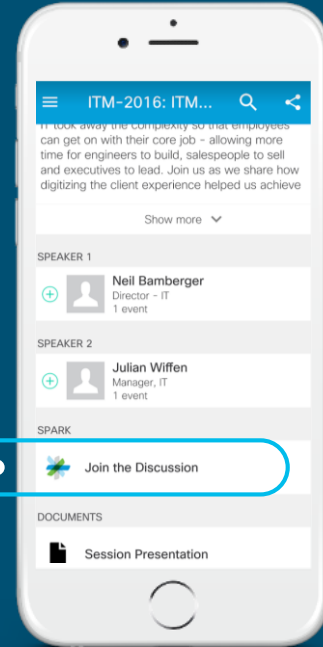


Questions?

Use Cisco Spark to communicate with the speaker after the session

How

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



Who is your Speaker?



- ned@cisco.com
- ~18 years @ Cisco / ~26 in Industry
- Security Architect for Large Global Companies
- CISSP #74780 | SFCE | CICSP (Web / Email)

- Background in Education, Healthcare, Retail and Energy
 - Security / Networking / Systems / Helpdesk
- Other sessions on ciscolive.com
 - Practical PKI for Remote Access (with ISE) – BRKSEC-2053/3053
 - Deploying PKI for Today's Networks (for 802.1x and VPN) – TECSEC-2053
 - Remote Access VPN with ASA (and FTD) - BRKSEC-2501
 - New for 2018-2019 - Uncovered: Detect and Protect from Hacking Tools

Agenda

- Endpoint Dilemma
- Security Capabilities
 - Incident Response
 - Prevention of Malware
 - Endpoint Behavior/Visibility
 - Network Blocking Malware
- Mapping to Threat(s)
- Summary



Session Details

What to expect

- Why endpoint is so important
- Endpoint capabilities from AnyConnect Umbrella Roaming, Network Visibility & AMP4E

What not to expect

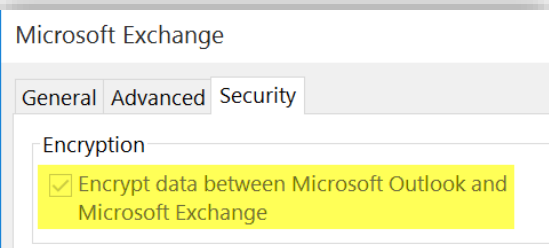
- Cover every endpoint feature, module in AnyConnect or other Cisco Endpoints

- If you see this  = Reference
- Policy controls of the endpoint are covered in the appendix
- Please see “Continuing Your Education” slide.

Endpoint Dilemma

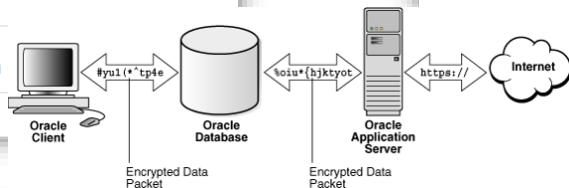
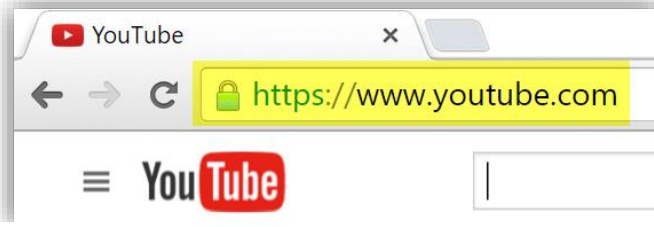
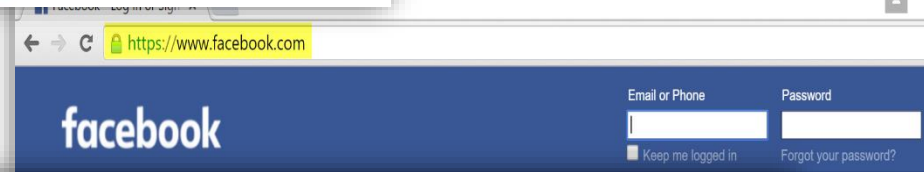
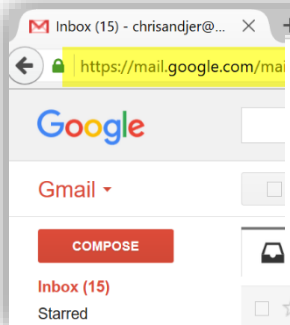


Everything is Encrypted!



User identification
☐ Always prompt for login

Logon network security:



Deciphering Malware's use of TLS (without Decryption)

Blake Anderson, Subharthi Paul, David McGrew

(Submitted on 6 Jul 2016)

The use of TLS by malware poses new challenges to network threat detection because traditional pattern-matching techniques can no longer be applied to its messages. However, TLS also introduces a



Supporting App Transport Security

December 21, 2016

App Transport Security (ATS), introduced in iOS 9 and OS X v10.11, improves user security and privacy by requiring apps to use secure network connections over HTTPS. At WWDC 2016 we announced that

What Encryption Problem?

- I can do “SSL/TLS” Decryption today, Right?

 Decrypt (Resign)	Valid	☐ HTTPS	☐ Secure Web browser	☐ Yahoo!	https://www.yahoo.com
 Decrypt (Resign)	Valid	☐ HTTP 2.0	☐ HTTP 2.0 client	☐ Google Hangouts	https://talkgadgets.google.com
 Decrypt (Resign)	Valid	☐ HTTP 2.0	☐ HTTP 2.0 client	☐ Google	https://clients6.google.com
 Decrypt (Resign)	Valid	☐ HTTPS	☐ SSL client	☐ Gmail	https://gmail.com
 Decrypt (Resign)	Valid	☐ HTTPS	☐ Secure Web browser	☐ Yahoo!	https://www.yahoo.com
 Decrypt (Resign)	Valid	☐ HTTPS	☐ SSL client	☐ Mozilla	https://tiles.services.mozilla.com
 Decrypt (Resign)	Valid	☐ HTTPS	☐ SSL client	☐ APNS	https://courier.push.apple.com
 Decrypt (Resign)	Valid	☐ SSL	☐ SSL client	☐ APNS	https://courier.push.apple.com

- Expensive on CPU on existing platform
- \$\$\$\$ Decryption Block
- What about the User Experience?

• TLS: HTTPS, mail transport (SMTP, IMAP)

• TLS: Hundreds of Pinned Applications

- Dropbox client, Google Drive
- iTunes
- Pokemon, SecondLife
- Chrome – Google Apps, Firefox, Opera
- WhatsApp
- Office 365 Mail
- Goto Meeting, Lync, Webex, Jabber

This list continues to grow!

• DTLS: WebRTC, DTLS-SRTP, Cisco AnyConnect

• IPsec: VPN

• Email Object encryption

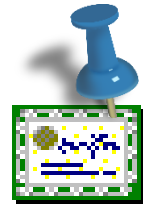
- PGP (Gmail, Yahoo), S/MIME (Apple iOS, Outlook)

• Application-layer encryption

- JOSE (javascript), WebCrypto, Enc. Push, Enc. Content-Encoding

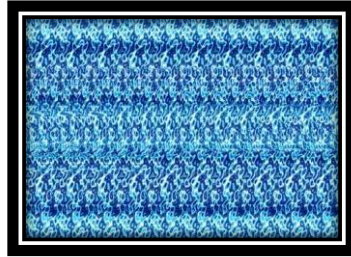
Proxy with TLS
client
cooperation

Un-breakable,
due to mutual
authentication
and/or certificate
pinning (HPKP)



Your Decryption Policy?

- Decrypt



- Permit

Not Decrypting

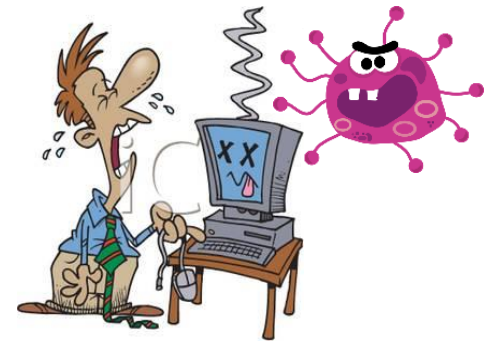
- Deny



- By leveraging AVC, URL Categories, Certificate – Common Name (CN)....etc
- Allowing something you shouldn't
- Blocking something you shouldn't

Device Security Problem

- Malware is still getting in, Why?
- Malware writers are testing against your tools
- They only have to be Correct 1 time
- Can I be 100% protected?



From: Melodie Mantooth <melodiekaipsxj947@outlook.com> ☆

Subject: Hey

To: victim@taointelligence.com <victim@taointelligence.com> ☆

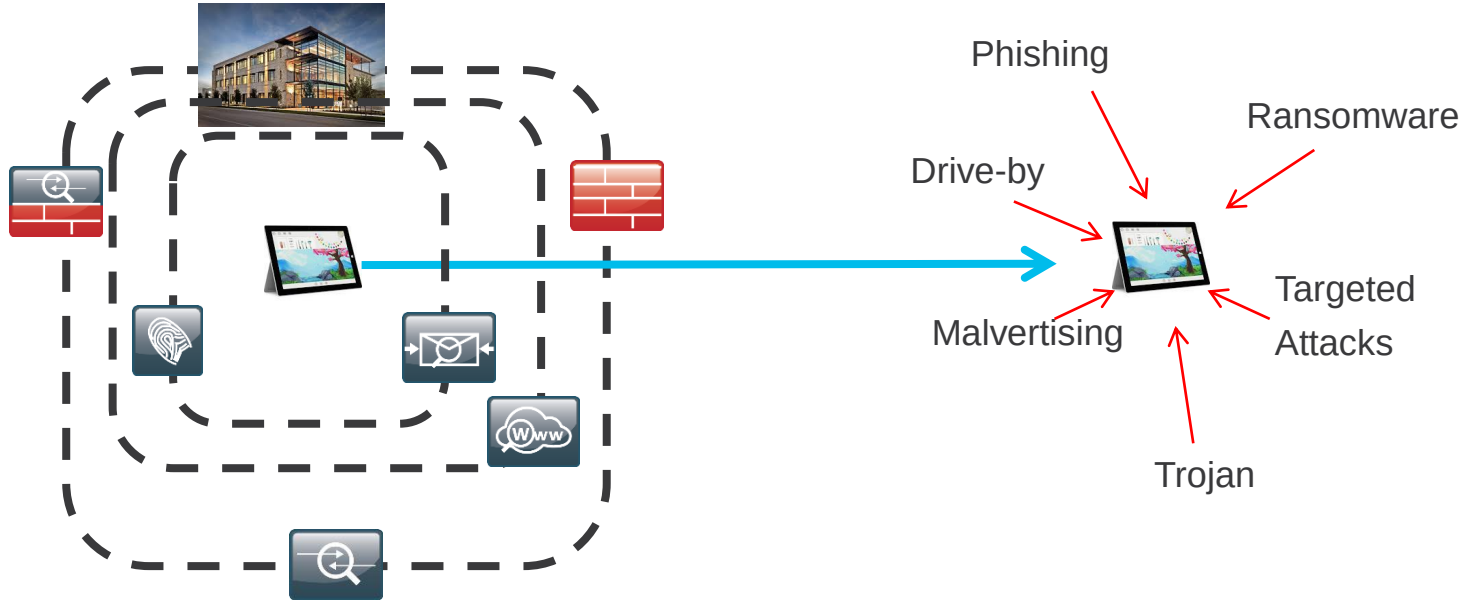
<https://www.google.com/url?hl=en&q=https://ef166ap2ffu2assu.onion.to/04562206.doc?id%3D41898248%26apr%3D1789&usp=DJCNEU13q30JMM3haq1dc8ZATHC0F9fQ>

Yours sincerely,
Alejandra



Endpoint = Last line of Defence, NOW First

- Devices are mobile now and leave the traditional Perimeter



Applications Good/Bad are in the Cloud



Every Application lived
in the DC/On premise



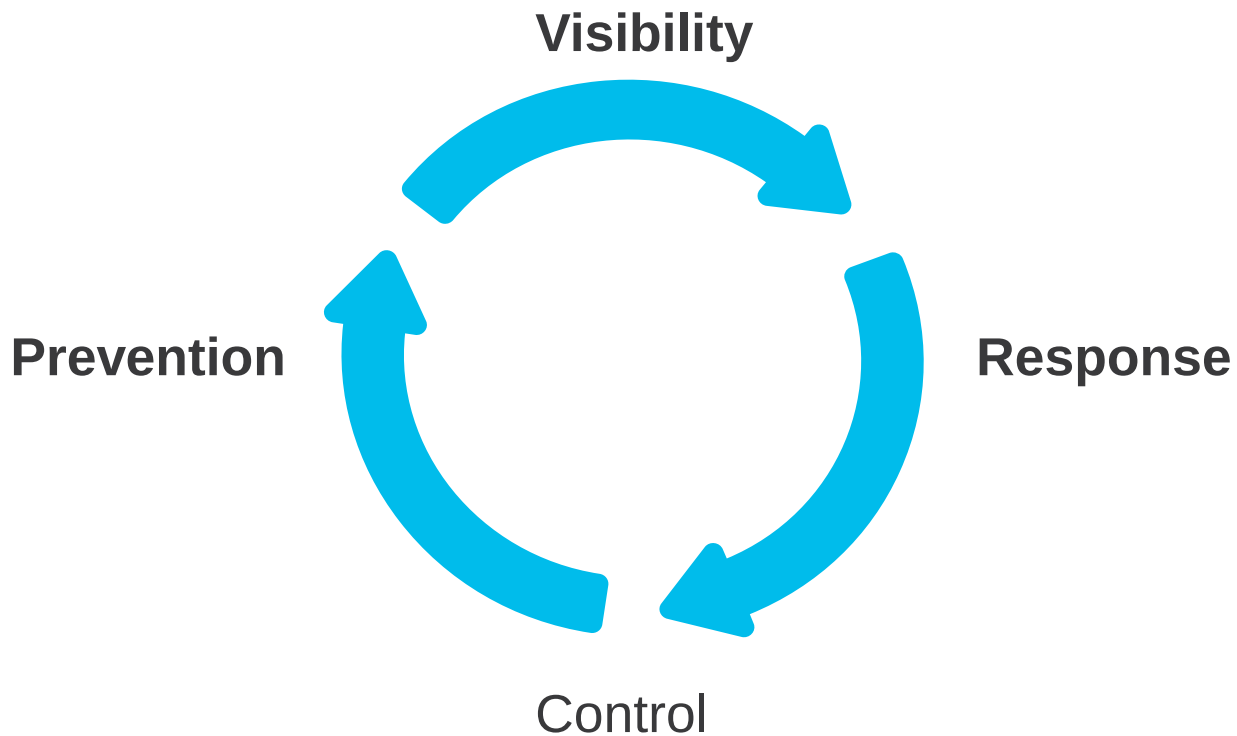
What to do?



*“What to do? **FOCUS on CAPABILITIES.** Don’t think “I need to shortlist me some EDR Vendors,” don’t think “my AV suck – I need EDR”, think **WHAT ENDPOINT SECURITY CAPABILITIES DO I NEED NOW?***

Gartner

What Endpoint Capabilities!



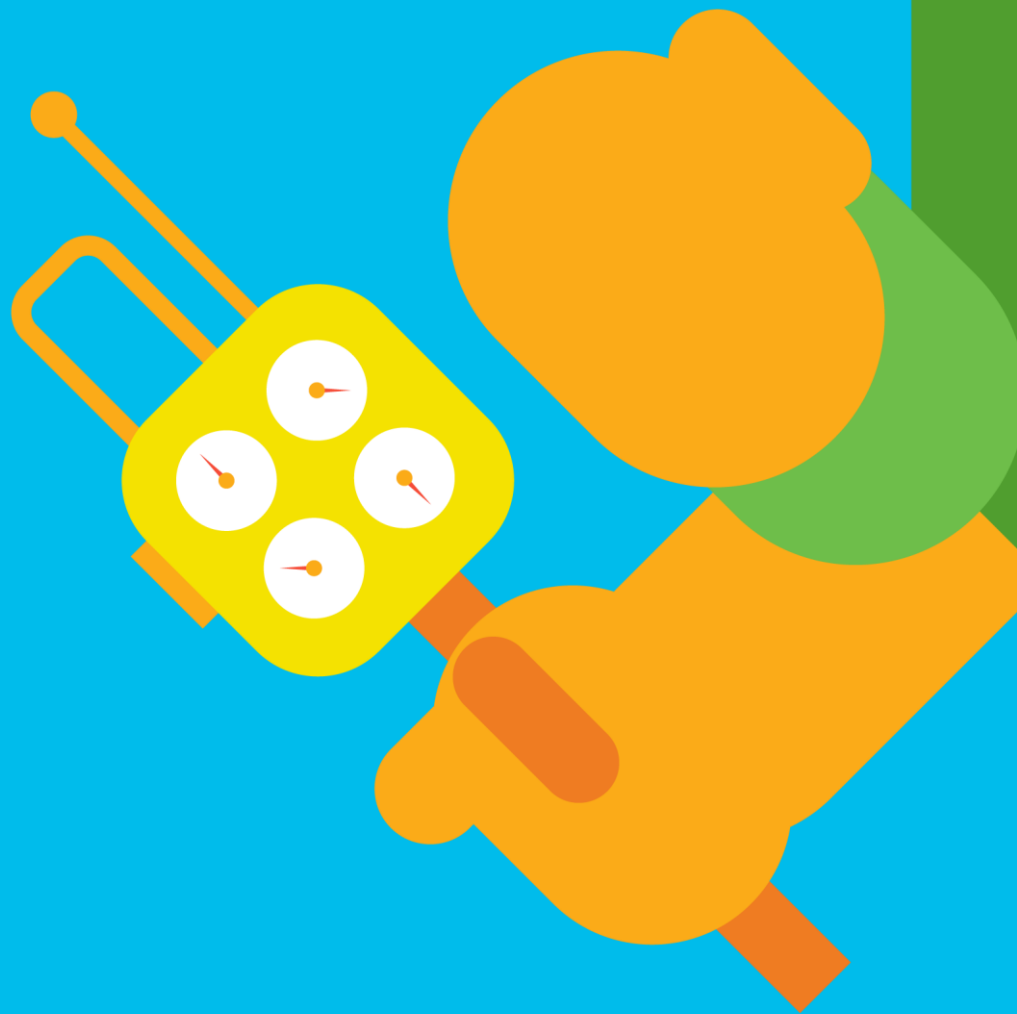
Agenda

~~• Endpoint Dilemma~~

- Security Capabilities
 - Incident **Response** - AMP
 - **Prevention** of Malware - AMP
 - Endpoint Behavior / **Visibility** – AnyConnect Network Visibility
 - Network Blocking Malware – AnyConnect Umbrella Roaming
- Mapping to Threat(s)
- Summary

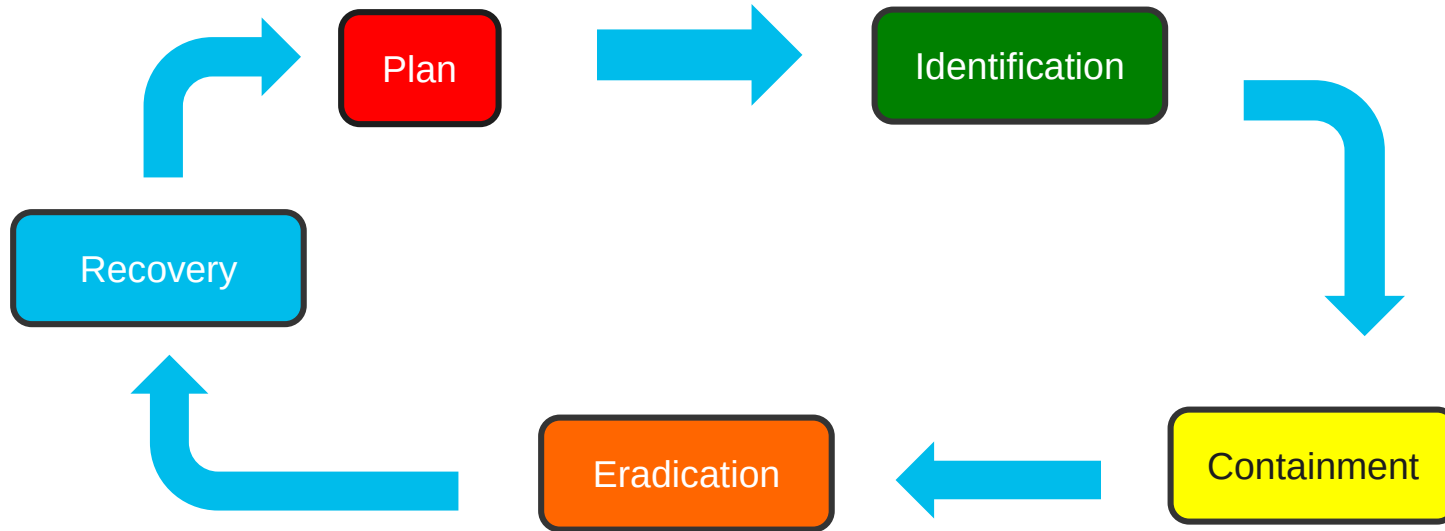


Incident Response



What is Incident Response?

- A process that involves an incident (a deviation from the normal usually because of a change in a system or network)!



<https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>

Identification

- Log files
- Security events when exists
- Eg. system acting strangely, error messages
- Who, What, Where, and How



What is Advanced Malware Protection for Endpoint (AMP4E)



- Cloud connected & managed (public or private)
- Focused on two modes of operation
 - Something I know → Prevention = Security Mode
 - **Something I don't know...yet → Retrospection = Incident Response Mode**

- Supported on



Cisco Security
Connector
Clarity*

- Deployed Standalone or AnyConnect Enabled - ISE or VPN

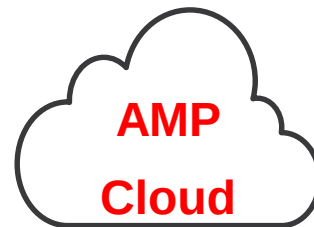
Visible Record

Identification



Connector records activity

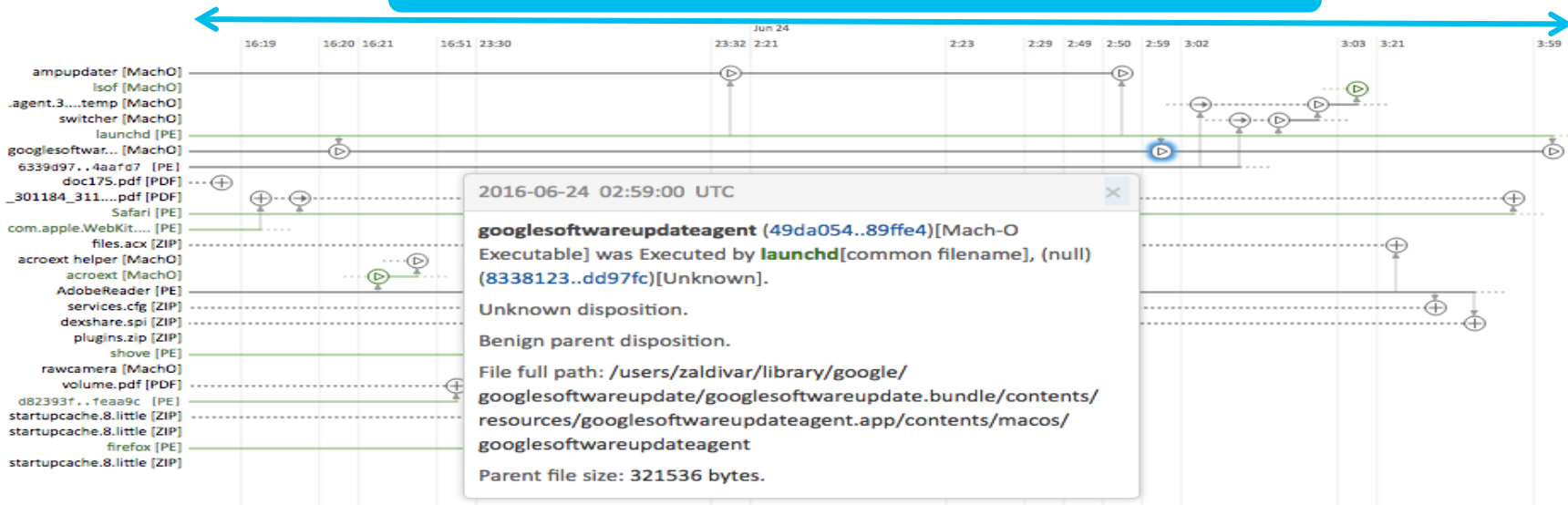
TCP 443



Device Trajectory

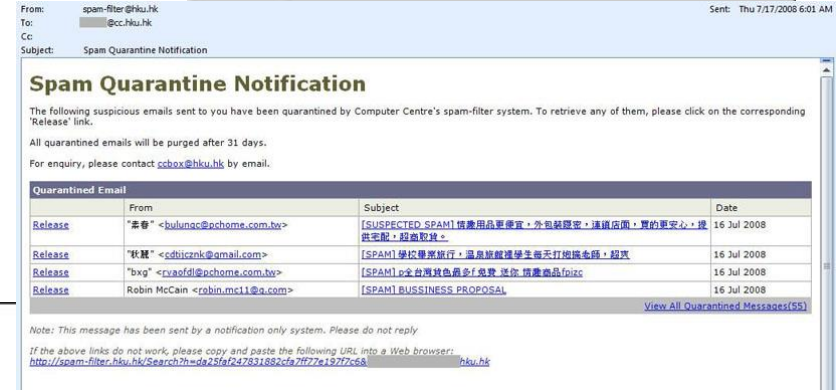
For Lisa Zaldivar's MacBook Pro

Visibility of Executions (History to Current)



What if There is No Alert?

- Something unusual – never seen before
- Vulnerable Software
- CMD Line – indicate tools or pivoting
- Scan for something specific



Prevalence – Low Execution Count

(Unique Files Worth Investigation)

Identification

The screenshot shows the FireAMP console interface with a list of files. The first entry is 'crashplanservice' which was only executed on 'nzaldiva-M-70SP'. The 'Analyze' button for this file is highlighted with a red box. A blue arrow points from a callout box to this button. Below this entry, there is a section for 'dropbox' which was only executed on 'nzaldiva-M-70SP'. This section includes a fingerprint (SHA-256) of '6d5344f8...0201be27', a list of computers (apple nzaldiva-M-70SP), and buttons for 'Device Trajectory' and 'File Trajectory'. The third entry is 'thnucInt' which was only executed on 'nzaldiva-M-70SP'.

File Name	Execution Location	Action	Timestamp
crashplanservice	apple nzaldiva-M-70SP	Analyze	2016-06-24 15:12:02 UTC
dropbox	apple nzaldiva-M-70SP	Analyze	2016-06-24 15:01:54 UTC
Fingerprint (SHA-256) 6d5344f8...0201be27			
Computers apple nzaldiva-M-70SP			
Device Trajectory File Trajectory			
thnucInt	apple nzaldiva-M-70SP	Analyze	2016-06-24 15:01:45 UTC

Analyse will trigger
Fetch if file not
already in repository

2Factor Required for
File Fetch

Authenticator

103 164

FireAMP Console (nzaldiva@cisco.com)

Vulnerable Software - Application <-> CVE

Identification

Dashboard

[Dashboard](#) [Inbox](#) [Overview](#) [Events](#) [Heat Map](#)

Filter: (New) ?

Select a Filter

Event Type **Vulnerable Application Detected**

Group All Groups

Filters Add filters by clicking on the icon in the event details

Time Range Week

Sort

Time

Not Subscribed

Reset

Save Filter As...

GBMacProServer executed Mozilla Firefox having 56 severe vulnerabilities

Vulnerable Application ...

2017-06-09 22:54:39 CDT

nzaldiva-M-70SP executed Oracle Java(TM) Platform SE having 2 severe vulnerabilities

Vulnerable Application ...

2017-06-08 14:25:46 CDT

Vulnerability Details

Connector Info

Comments

Fingerprint (SHA-256)

Filename

Application

java

Oracle Java(TM) Platform SE, Version:1.8.0:update_101

CVE-2016-5573 6.8

CVE-2016-5582 9.3

[View Upload Status](#) [File Trajectory](#)

Vulnerable Software - Application <-> CVE

Identification

CVEs identified for application

Individual Scores for each Application

☐ Mozilla Firefox v45.0.2	8975bb5a...16175805	☐ 3	5 severe vulnerabilities	2016-05-11 22:20:32 UTC	10.0
CVE-2016-2804 ☐ 10.0	CVE-2016-2806 ☐ 10.0	CVE-2016-2807 ☐ 10.0	CVE-2016-2811 ☐ 6.8	CVE-2016-2814 ☐ 6.8	
Observed in groups: CSS-Devices nzaldiva_devices Laptops					
Filename: firefox					
Last observed: ☐ Lisa Zaldivar's MacBook Pro • 2016-05-11 22:20:32 UTC • ☐ Device Trajectory					

Command Line Visibility

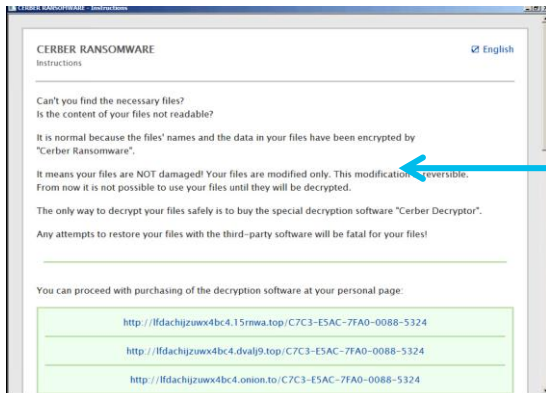
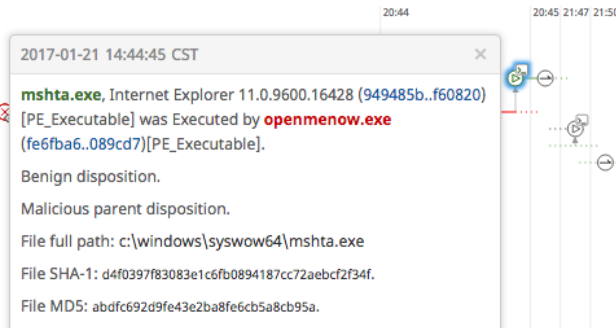
Device Trajectory

w7pc-corp.demo.local

Identification

```
[ System ]
ed09eb2e8....zip [ZIP]
mshta.exe [PE]
cmd.exe [PE]
openmenow.exe [PE]
acumbrella....exe [PE]
services.exe [PE]
svchost.exe [PE]
```

Example of Ransomware displaying Instructions for payment



Command line

CWD

CMD C:\Windows\SysWOW64\mshta.exe
C:\Users\admin.DEMO\AppData\Local\Temp\README.hta

Environment variables

USERNAME admin

Pivoting
Tools
File-less malware

Device Trajectory – Examine Suspicious

services.cfg [ZIP]

301184_311 Adobe 419c2f4..c6184d

zaldivarpsyc dexsh

attachments mrpch03-fro

desantastatio quotation - lis

zaldiv letter638649

pediatric anx proposal-win

63596157577 anxiety pedia

brinson - par brinson - par

estimate of r 301184_311

301184_311 valdiv

adobeflashpla creditcardap

fa phone list fa phone list j

brinson - par clientracke

Disposition: Unknown

Filename: services.cfg

File not on VirusTotal

VirusTotal

Copy SHA-256

Search

View Full SHA-256

File Analysis

File Trajectory

File Fetch

Simple Detection

Application Blocking

Whitelist

Is it known by Cisco?

Compare with 3rd party

Dig Deeper

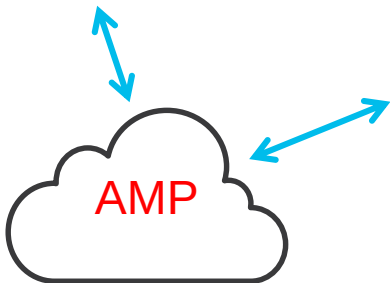
- Analyse with ThreatGrid
- File Details and Network Profile
- Retrieve File

Take action

- Detect and Quarantine
- Detect – Block execution
- Allow

Detailed File Analysis from ThreatGrid

Identification



File Analysis

For **3372c1ed...c234a370**

[Download Sample](#) [Analysis Video](#) [Download PCAP](#) [767 Artifacts](#)

ThreatGRID
Full-Scale Threat Intelligence Platform

[Metadata](#) [Behavioral Indicators](#) [Network Activity](#) [Processes](#) [Artifacts](#) [Registry Activity](#) [File Activity](#)

Analysis Report

ID	d0a50a9d03f22022426468a3c6b5ff00
OS	2600.xpsp.080413-2111
Started	2/4/16 12:32:10
Ended	2/4/16 12:39:01
Duration	0:06:51
Sandbox	phl-work-04 (pilot-d)
Filename	0719738791.exe
Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows
Analyzed As	exe
SHA256	3372c1edab46837f1e973164fa2d726c5c5e17bcb888828ccd7c4dfcc234a370
SHA1	e654d39cd13414b5151e8cf0d8f5b166ddd45cb
MD5	209a288c68207d57e0ce6e60ebf60729

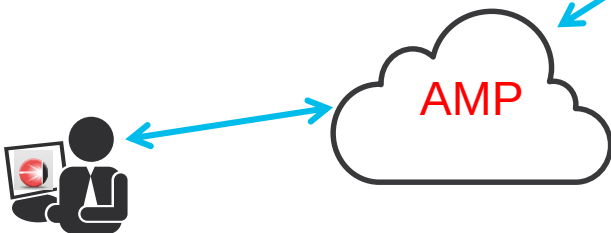
Behavioral Indicators

Shadow Copy Deletion Detected	Severity: 100	Confidence: 100
Process Modified Desktop Wallpaper	Severity: 100	Confidence: 95
Process Modified a File in a System Directory	Severity: 90	Confidence: 100
Artifact Flagged as Known Trojan by Antivirus	Severity: 100	Confidence: 85
Process Modified a File in the Program Files Directory	Severity: 80	Confidence: 90
Process Modified an Executable File	Severity: 60	Confidence: 100
Process Created an Executable in a User Directory	Severity: 60	Confidence: 95
Process Modified File in a User Directory	Severity: 70	Confidence: 80
Artifact Flagged by Antivirus	Severity: 50	Confidence: 50

Easy classification by using Severity (**95+ Bad, 70+ suspicious**) and Confidence Threat Scoring

Endpoint IoC Scan

- IoC = Indicator of Compromise
- Based on OpenIoC 1.1
- Primary use case is IR
- Secondary Correlated Scans

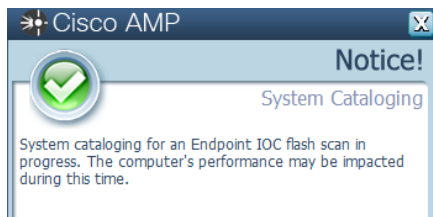


Created XML File using Editor

← → ↺ ⓘ openioc.org/iocs/ea3cab0c-72ad-40cc-abbf-90846fa4afec.ioc

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  abbf-90846fa4afec" last-modified="2011-11-04T19:35:05">
  <short_description>STUXNET VIRUS (METHODOLOGY)</short_description>
  <description>
    Generic indicator for the stuxnet virus. When loaded, stuxnet spawns lsass.exe in a suspended state.
    CONTEXT to point to the newly mapped in section. This is a common task performed by malware and allo
    process.
  </description>
  <keywords>methodology</keywords>
  <authored_by>Mandiant</authored_by>
  <authored_date>0001-01-01T00:00:00</authored_date>
  <links/>
  <definition>
    <Indicator operator="OR" id="73bc8d65-826b-48d2-b4a8-48918e29e323">
      <IndicatorItem id="b9ef2559-cc59-4463-81d9-52800545e16e" condition="contains">
        <Context document="FileItem" search="FileItem/PEInfo/Sections/Section/Name" type="mir"/>
        <Content type="string">.stub</Content>
      </IndicatorItem>
      <IndicatorItem id="156bc4b6-a2a1-4735-bfe8-6c8dlf7eae38" condition="contains">
        <Context document="FileItem" search="FileItem/FileName" type="mir"/>
        <Content type="string">mdmcpq3.PNF</Content>
      </IndicatorItem>
    </Indicator>
  </definition>
</ioc>
```



Endpoint IoC Example – Dridex5.Talos.ioc

·AND

- File Full Path contains C:\Documents and Settings
- File Import Name is pdh.dll
- File Import Name is SHELL32.dll
- File Import Name is KERNEL32.dll

☐ OR

- File Name contains edg
- File Name contains .exe

☐ OR

- File Full Path contains Local Settings\Application Data\
- File Full Path contains AppData\Local\

logical operators AND/OR

FilePath

Specific DLLs

Filename extensions



Endpoint IoC Details

	Running Processes	Loaded DLLs	Services	Drivers	Task Scheduler	Sys Info	User Account Info	Browser History & Downloads	Windows Event	Network & DNS Info	Registry	Files & Dir	Sys Restore Points
Flash	X	X	X	X	X	X	X	X	X	X			
Full	X	X	X	X	X	X	X	X	X	X	X	X	X

IoC Attributes & IoC Examples->

<https://docs.amp.cisco.com/Cisco%20Endpoint%20IOC%20Attributes.pdf>

Recommendations:

- If you do not have a full catalog the endpoint, scan will return nothing
- Flash Scan very quick, couple of minutes, Full scan can take 1-2 hours.

Cisco *live!*

2018-03-01 15:29:05 CST

Flash scan started by the UI.

Scan completed successfully.

Found 0 detections and 0 suspicious files.

Scan time 1 minutes.

Scanned 1133 files, 5 directories and 0 processes.

Engines used: SHA, ClamAV.

Endpoint IoC Demo

Summary of IR Response Actions

- Simple Detection -> Detect/Quarantine
- Application Blocking – Block Execution of Vulnerable Applications
- Blacklist – Blocking C2 or further distribution, Recommendation is use Umbrella
- Prevalence -> Analysis of File
- Endpoint IoC -> Look for something specific

Prevention of Malware

When you think Prevention?

- Signature/Algorithm – typically associated with Antivirus

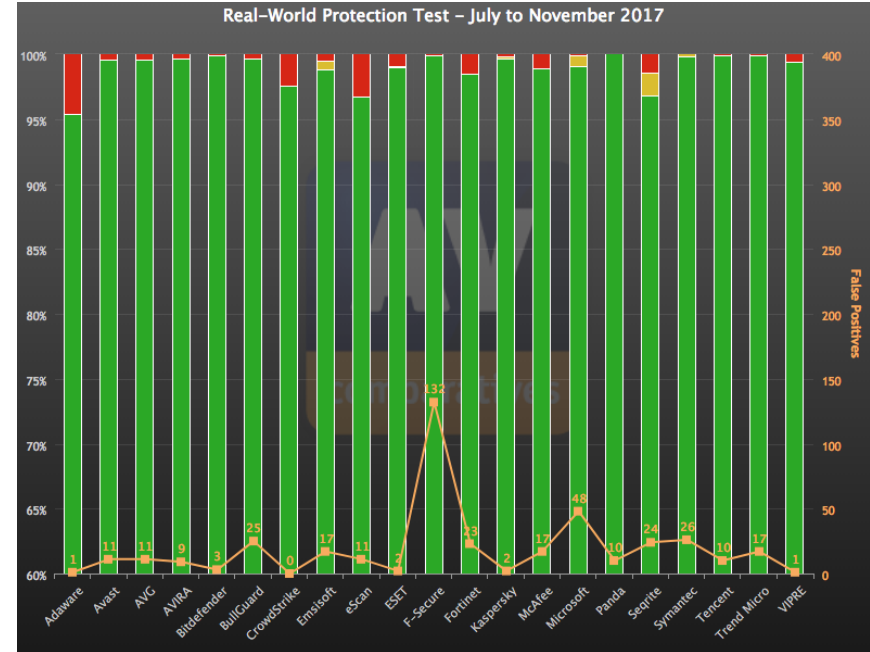
OR

- Advanced Malware Engine – leveraging Cloud DB/Analytics



A Look Deeper at Anti-Virus?

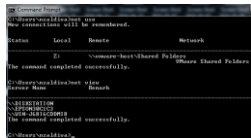
- What it includes:
 - Anti-malware is included
 - Signatures - > Not Complete DB, Often Retired
 - Set of Algorithms
 - Remediation engine
 - Differential updates
- Most provide same level of protection
- Image from AV Comparatives Nov. 2017 ->



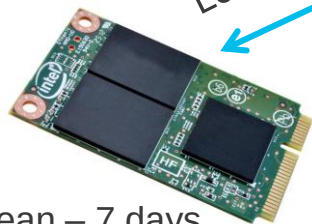
AMP for Endpoint - Inside



1 Copy, Move, Execute, Create, CLI...

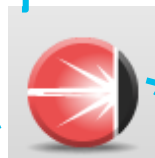


3 Lookup in Cache



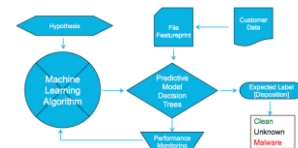
Clean – 7 days
Unknown – 1hr
Malware – 1hr
(modifiable)

Cisco *live!*



2 1-1 SHA-256 Hash
Spero Fingerprint
(machine learning)

6e693146...303862cd



4 ETHOS (fuzzy logic) / DFC
443 – lookup ~200ms / 540b



Low Prevalence or Analysis



7 Exploit Prevention
(memory injection)



Custom Detection



Tetra/ClamAV

AMP for Endpoint - Inside



- **1-1 SHA-256 Check** – cloud lookup against 8+ years of malware (Millions of samples)
- **Spero** – Examines PE headers, DLL imports, Compile location, 400 Factors, compares those against known bad to give probability – **machine learning based**
- **Ethos** – attempts to pack/unpack/repack to match existing hash, enabled by default for copy/move – fuzzy logic based, CPU intensive. – Groups Files together allows detection of remediation of variants for malware families.
- **Device Flow Correlation** – kernel view at Network I/O. Allows blocking or alerting, traced back to process. Cisco provided intelligence and Custom supported.
- **Exploit Prevention** – protection into memory injection attacks, block but no quarantine.
- **clamAV**- helps with unpacking and file type identification, detect/quarantine, AV Engine on Mac
- **Tetra** – AV database, primarily focused on off-line protection, last line of defence.

Detection / Quarantine on Endpoint

Warning!
Threat Detected

openmenow.exe has been detected as W32.FE6FBA6041-100.SBX.TG.

File History

View By: Default | 12/7/2016 31 | 12/14/2016 31 | keyword

Event	File Name	Date
🔒		12/14/2016 8:21:48 AM
✅	WdfCoInstaller01009.dll	12/14/2016 7:46:49 AM
✅	difxapi.dll	12/14/2016 7:46:49 AM
✅	casetup64.exe	12/14/2016 7:46:48 AM
✅	global_25D1963E-EDBF-4486-A2A0-A714A407D874.xml	12/14/2016 7:46:48 AM
✅	UserInfo.dll	12/14/2016 7:46:48 AM
✅	dcl.dll	12/14/2016 7:46:47 AM
✅	global.xml	12/14/2016 7:46:47 AM
✅	libeay32.dll	12/14/2016 7:46:47 AM
✅	msvcp100.dll	12/14/2016 7:46:47 AM
✅	msvcr100.dll	12/14/2016 7:46:47 AM

Details
Event Type
Quarantine Successful
Detection Name
Gen:Variant.Razy.108073
File Path

Date
12/14/2016 8:21:48 AM

Close

- AMP Naming Conventions

<http://www.talosintelligence.com/amp-naming/>

- Quarantine folder is where quarantined files are stored
- Renamed qrt<sha>. [0-9] [0-9] [0-9]
- Files can be restored < 30days

Detection/Quarantine on Endpoint – Management View

Malware Threats (7 days)

Detection Name	Count
----------------	-------

W32.DFC.MalParent	232
-------------------	-----

GenericKD:Dyreza-tpd	68
----------------------	----

W32.File.MalParent	30
--------------------	----

W32.ZAccess.15nt	26
------------------	----

W32.Ramnit.A	14
--------------	----

2016-12-14 08:21:48 CST

Detected **Gen:Variant.Razy.108073** as **exe** (93df7cf..6aa06e)[PE_Executable] during a full s
The file was quarantined.

File size: 306176 bytes.

File age: 0 seconds.

Detected by the Tetra engines.

Elevated on
Dashboard as an
IoC, Network or
Malware Threat.

SHA-256

Result – Quarantine,
Not Quarantined

Engine Identified –
SPERO, ETHOS,
TETRA...etc

Endpoint Behavior/ Visibility

What is Netflow or IPFIX

- IPFIX is a IETF Standard (RFC 7071) version of Neflow.



Flow Information	Packets
SOURCE ADDRESS	10.1.8.3
DESTINATION ADDRESS	172.168.134.2
SOURCE PORT	47321
DESTINATION PORT	443
INTERFACE	Gi0/0/0
IP TOS	0x00
IP PROTOCOL	6
NEXT HOP	172.168.25.1
TCP FLAGS	0x1A
SOURCE SGT	100
:	:
APPLICATION NAME	NBAR SECURE-HTTP

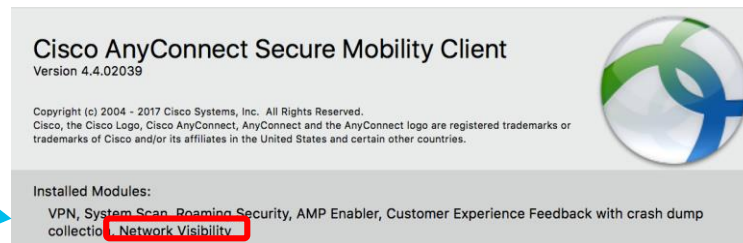




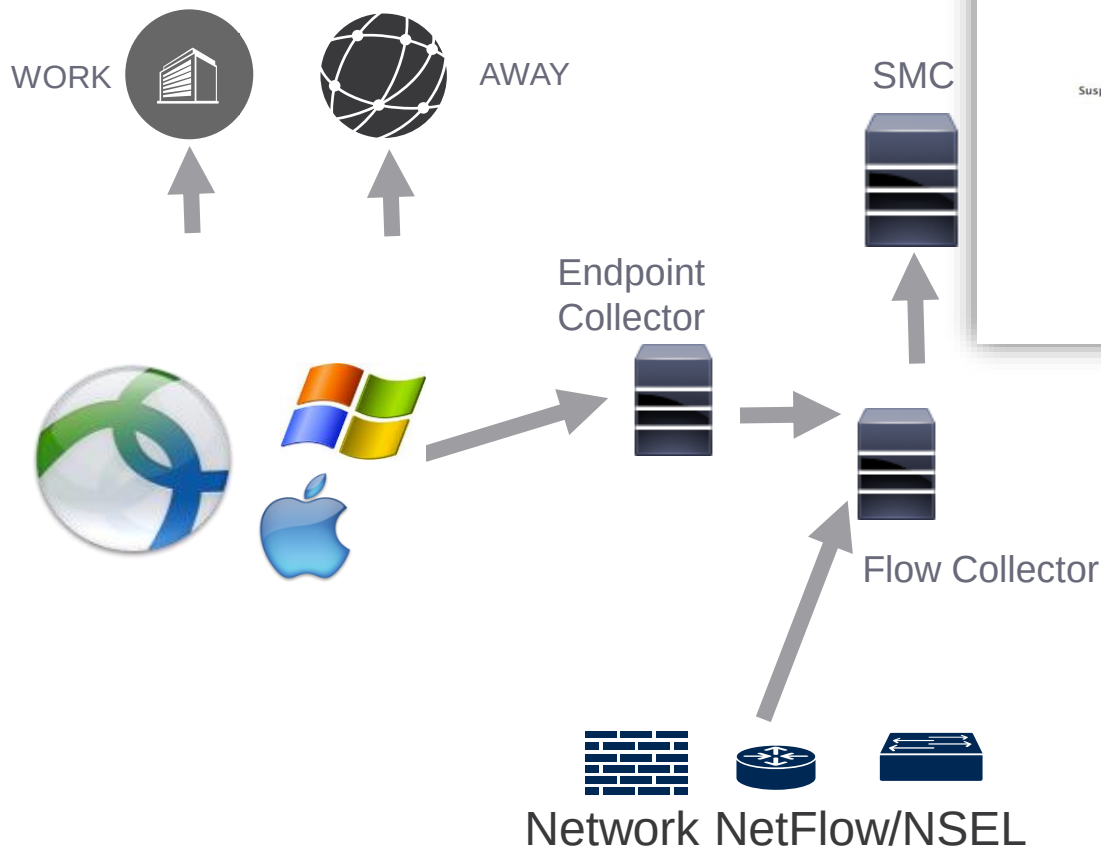
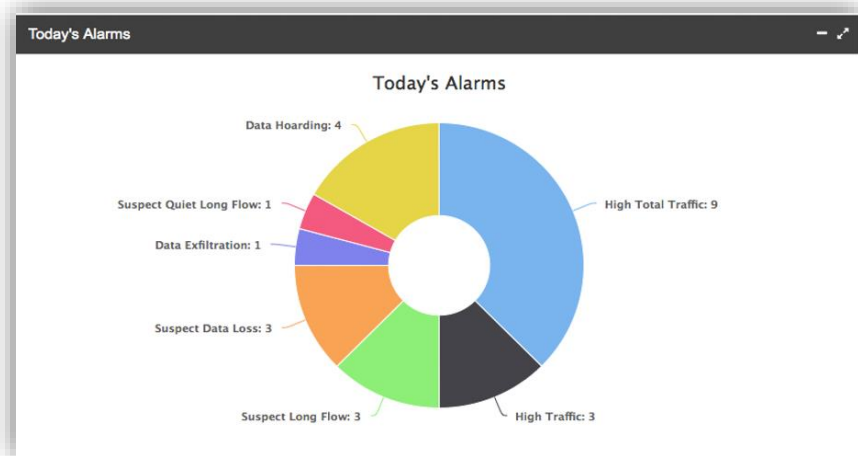
AnyConnect Network Visibility Module



-  for 4.2MR1 – 4.2.1022
- Supported on Windows and Mac devices
- Hidden Module
- Apex License Required
- Integration with Stealthwatch 6.8+, LiveAction, Splunk (Enterprise 6.0 with Collector 64-bit Linux) and Plixer (not official), IBM Qradar and Exabeam



NVM with Stealthwatch

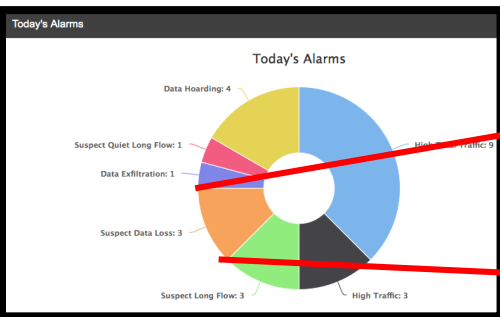


Context

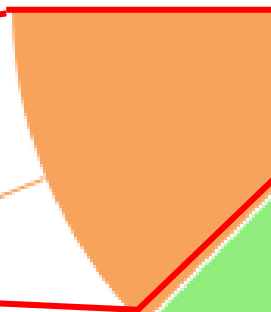
- User
- Application
- Device
- Location: To / From

to Existing Alarms and Flow Data*

Data Loss from Stealthwatch Console



Suspect Data Loss: 3



Alarms : Suspect Data Loss for Today (4)

Alarms

First Active	Source Host Groups	Source	Target Host Groups	Target	Alarm	Policy	Event Alarms	Source User	Details	Last Active	Active	Acknowledged
12/21/15 6:10 PM	Remote VPN IP Pool	172.16.31.14	--	Multiple Hosts	Suspect Data Loss	Client IP Policy	--	--	Observed 521.57M bytes. Un-baselined Host. Policy maximum allows up to 500M bytes.	Current	Yes	No

HTTPS Unclassified Identified, Is that helpful?

Application	Total	%	Sent	Ratio	Received	7-day Trend
HTTPS (unclassified)	213.07MB	94.00	192.8MB		20.28MB	

Host Summary



Host IP
172.16.31.14

View Flows

Classify

History

Status: Active

Hostname: --

Host Groups: Remote VPN IP Pool

Location: RFC 1918

Last Seen: 12/21/15 6:48 PM

Policies: Client IP Policy, Inside

MAC Address: --

Application Traffic							Internal	External
Application	Total	%	Sent	Ratio	Received	7-day Trend	24-hour Trend	
HTTPS (u...	213.07MB	94.00	192.8MB		20.28MB			
HTTP (uncl...	6.53MB	3.00	630.14KB		4.96MB			
Undefined...	6.6MB	3.00	108.22KB		6.6MB			
NTP (uncl...	192B	< 0.01	96B		96B			
NetBIOS (...)	30.68KB	< 0.01	30.68KB		0B			
DNS (uncl...	6.02KB	< 0.01	1.97KB		4.05KB			

5:00 PM
Outbound: 192.8MB
Inbound: 20.28MB

HTTPS Unclassified Now Known!

AnyConnect NVM provides IPFIX+

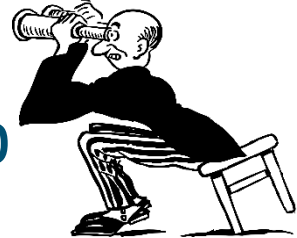


Start	End	Duration	Subject Orientation	Subject IP Address	Subject NAT	Process Name
Dec 21, 2015 5:57:48 PM	Dec 21, 2015 6:16:59 PM	19m 11s	Client	172.16.31.14	10.0.0.6	Dropbox

- Application Identified – Dropbox
- Application Hash – Who else is running?
- Identity – nedzaldivar (even without ISE or Identity, from non domain asset)

File Hash	Process Username	Connection Application
8B46902FE7A294A1F59EC830122161540A527726D72900E6534D39AA7723E523	Neds-MacBook-Pro.local/nedzaldivar	HTTPS (unclassified)

Verify Application is Correct Using Hash Lookup

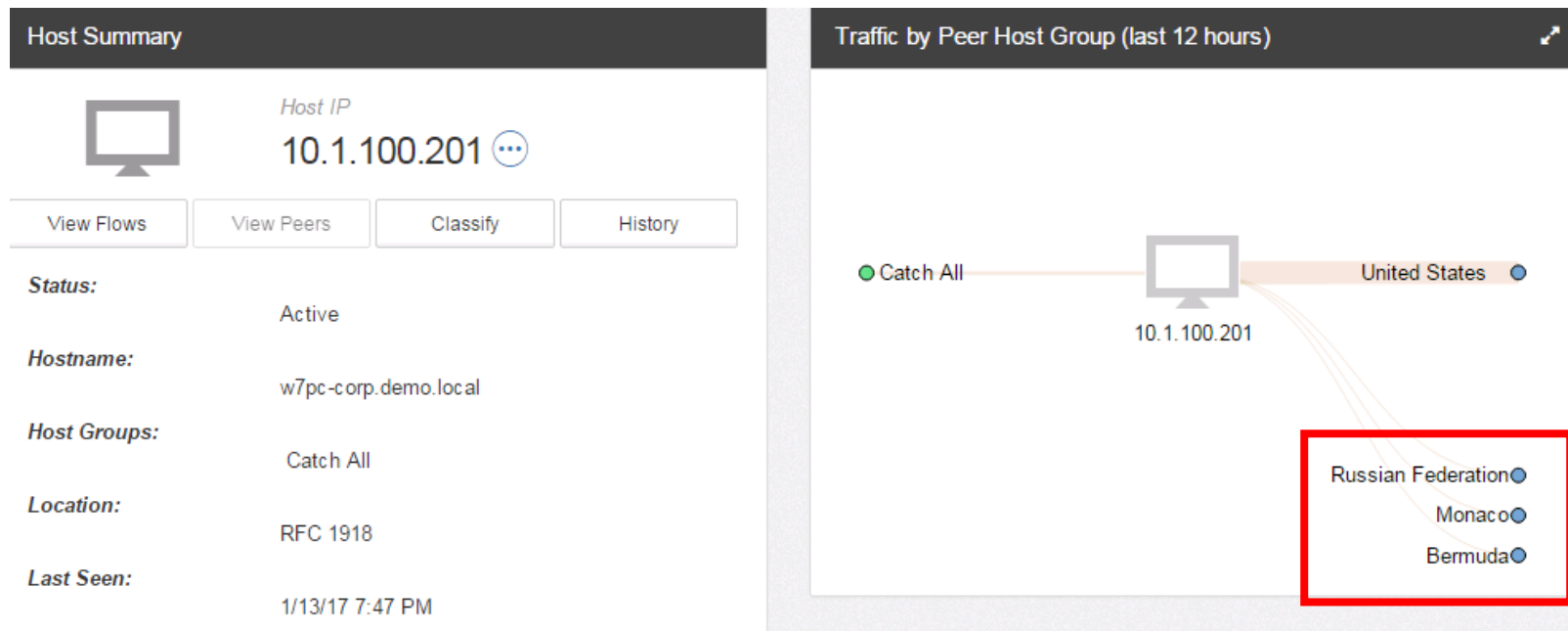


Start	End	Duration	Subject Orientation	Subject IP Address	Subject NAT	Process Name
Dec 21, 2015 5:57:48 PM	Dec 21, 2015 6:16:59 PM	19m 11s	Client	172.16.31.14	10.0.0.6	Dropbox

File Hash	Process Username	Connection Application
8B46902FE7A294A1F59EC830122161540A527726D72900E6534D39AA7723E523	Neds-MacBook-Pro.local\nedzaldivar	HTTPS (unclassified)

SHA256:	8b46902fe7a294a1f59ec830122161540a527726d72900e6534d39aa7723e523
File name:	File signature
Detection ratio:	Identifier com.getdropbox.dropbox
Analysis date:	Format mach-o thin (600)
	CDHash 105b743dcfa963d07d4b92466190674525307620
	Signature size 8511
	Authority Developer ID Application: Dropbox, Inc.
	Authority Developer ID Certification Authority
	Authority Apple Root CA
	Timestamp Dec 8, 2015, 9:34:17 PM
	Info.plist not bound
	TeamIdentifier G7HH3F8CAK
	Sealed Resources none
	Interesting properties
	This file is signed by Apple's Root Certificate Authority.

Another Scenario: Investigate Geolocation Data?



Flows to Russia and Monaco

Start: 01/21 - 08:44:12 PM End: 01/21 - 08:46:33 PM Duration: 2m 21s	 10.1.100.201 ⓘ RFC 1918	59390/UDP	53B 4 packets → Undefined UDP ← 0B 0 packets	6892/UDP	 194.165.18.0 ⓘ Russian Federation
Start: 01/21 - 08:44:12 PM End: 01/21 - 08:46:33 PM Duration: 2m 21s	 10.1.100.201 ⓘ RFC 1918	59390/UDP	53B 4 packets → Undefined UDP ← 0B 0 packets	6892/UDP	 194.165.18.254 ⓘ Russian Federation
Start: 01/21 - 08:44:12 PM End: 01/21 - 08:46:34 PM Duration: 2m 22s	 10.1.100.201 ⓘ RFC 1918	59390/UDP	53B 4 packets → Undefined UDP ← 0B 0 packets	6892/UDP	 194.165.19.254 ⓘ Russian Federation
Start: 01/21 - 08:44:12 PM End: 01/21 - 08:46:31 PM Duration: 2m 19s	 10.1.100.201 ⓘ RFC 1918	59390/UDP	53B 4 packets → Undefined UDP ← 0B 0 packets	6892/UDP	 194.165.17.254 ⓘ Monaco
Start: 01/21 - 08:44:21 PM End: 01/21 - 08:45:22 PM Duration: 1m 1s	 10.1.100.201 ⓘ RFC 1918	58754/UDP	24B 1 packets → Undefined UDP ← 0B 0 packets	6892/UDP	 194.165.19.254 ⓘ Russian Federation
Start: 01/21 - 08:44:19 PM End: 01/21 - 08:45:21 PM Duration: 1m 2s	 10.1.100.201 ⓘ RFC 1918	58754/UDP	24B 1 packets → Undefined UDP ← 0B 0 packets	6892/UDP	 194.165.18.254 ⓘ Russian Federation
Start: 01/21 - 08:44:17 PM End: 01/21 - 08:45:19 PM Duration: 1m 2s	 10.1.100.201 ⓘ RFC 1918	58754/UDP	24B 1 packets → Undefined UDP ← 0B 0 packets	6892/UDP	 194.165.17.254 ⓘ Monaco

Click Here

Using Chrome Extension Lookup Hash for Verification

Flow Detailed Summary: 10.1.100.201

Search Subject Details

Packets:
4
Packet Rate:
0.03pps
Bytes:
53B
Byte Rate:
0.38bps
Percent Transfer:
100.00%
Host Groups:
Catch All
Process Name:
openmenow.exe
File Hash:
FE6FBA6041293C2ADA6850841D77B1049450D174DD0CF53F4...
3F481B8F06...
Parent File Hash:
0000000000...
0000000000...

Totals

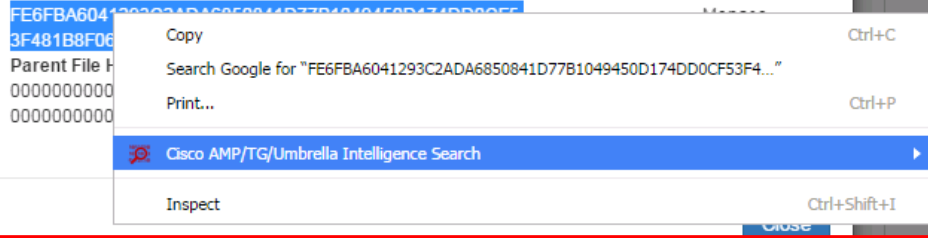
Packets:
4
Packet Rate:
0.03pps
Bytes:
53B
Byte Rate:
0.38bps
Subject Byte Ratio:
100.00%
RTT:
0s
SRT:
0s

Peer Details

Packets:
0
Packet Rate:
0pps
Bytes:
0B
Byte Rate:
0bps
Percent Transfer:
0.00%
Host Groups:
Catch All

Chrome Extensions for lookups, just a right click away

- VirusTotal
- ThreatGrid
- Umbrella



Unknown Application Identified-Cerber Ransomware

Analysis Report

[Resubmit](#)

ID ed09eb2e8058d6a5c85bb2c06e25812b
OS 2600.xpsp.080413-2111
Started 1/11/17 17:52:04
Ended 1/11/17 17:59:59
Duration 0:07:55
Sandbox car-work-037 (pilot-d)

Filename fe6fba6041293c2ada6850841d77b1049450d174dd0cf53f481b8f06a0089c
d7.exe
Magic Type PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Analyzed As exe
SHA256 fe6fba6041293c2ada6850841d77b1049450d174dd0cf53f481b8f06a0089cd7
SHA1 7cf92e2c1b21620c4fffb2d5ba34fda6a8b549502
MD5 db53d6d8f830b12eee7de4660689378a
Tags [tag](#)

Behavioral Indicators

Threat Score: 100

+ Ransomware Backup Deletion Detected	Severity: 100 Confidence: 100
+ Cerber Ransomware Detected	Severity: 100 Confidence: 100
+ WMIC Used to Delete Shadow Copy	Severity: 95 Confidence: 100
+ Artifact Flagged Malicious by Antivirus Service	Severity: 100 Confidence: 95
+ Process Modified Desktop Wallpaper	Severity: 100 Confidence: 95

Network Block Malware



Network Block Malware Option Comparison

DNS Intelligence

- Allows you to see DNS calls
- Very lightweight, no latency
- No scanning engines, big data used to determine what is good and bad.

Proxy Traffic

- Allows you to see all traffic
- Added latency
- Support for Micro-categories or behaviors. Like, Post, Upload
- Bandwidth throttling
- Requires multiple scanning engines to determine if Malware, C2, Ransomware, Dropper site..etc

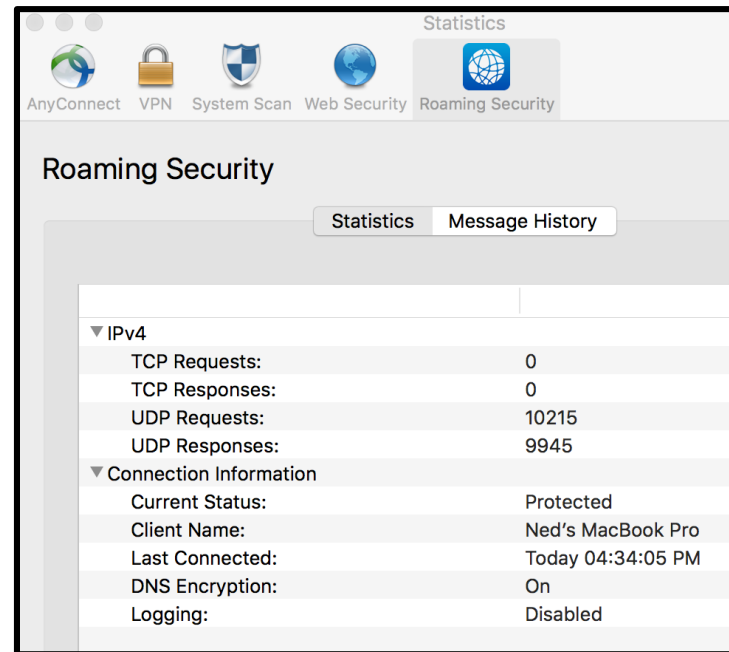
What is AnyConnect Umbrella Roaming Client?



- Off Trusted network protection across all ports for both Domain and IP
- Added layer of protection for existing security controls



- AnyConnect 4.3+ (Windows / Mac)
- Cisco Security Connector - iPad/iPhone*



Umbrella - How does it work?

Encrypted

Authenticated

DNS/IP Security Filtered



443 (QUIC) or
53



53



208.67.222.222
208.67.220.220

On Trusted Network
Client goes dormant
Network is Protected



Local Corp DNS

First Match Rule Table by Identity

1	AD User Policy: Bandwidth Hogs + Security + Log All Events	Impacting 55 Identities	Category Setting Default Settings	Security Setting All Security Protect...
2	Abuse Containment	Impacting 5 Identities	Whitelist-only mode	
3	Guest Policy (non AD users & BYOD): High Web Filtering + S...	Impacting 2 Identities	Category Setting High Web Filtering	Security Setting All Security Protect...
4	Executive Policy: No Web Filtering + Security + Log Security ...	Impacting 3 Identities	Category Setting No Web Filtering	Security Setting All Security Protect...
5	Marketing Policy: Access to Facebook	Impacting 6 Identities	Category Setting High Web Filtering	Security Setting All Security Protect...
6	At Home Laptop Policy: No Web Filtering + Security + Loggi...	Impacting 31 Identities	Category Setting No Web Filtering	Security Setting All Security Protect...
7	Default Policy	Impacting All Identities	Category Setting High Web Filtering	Security Setting All Security Protect...



Root/SP DNS

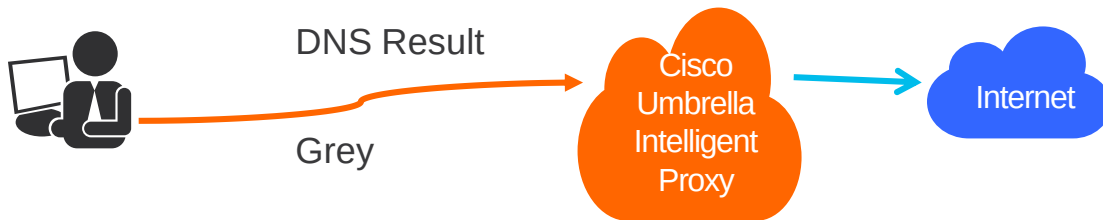
Intelligent Proxy

Normally DNS to IP address is returned



Umbrella makes decision on what to proxy

but when the value is GREY, Then Intelligent proxy kicks in and proxies the traffic



Options

- Block page
- SSL Decryption (Certificate available for download and distribution)
- File Inspection – AV and AMP

Incident Response Blocking – Destination List

Define
Destination
List



Block a
Specific
domain



Roaming Computers Block List		Type	Domains	IPs	URLs	Last Modified
		Blocked	1	0	0	Mar 3, 2018

List Name

Destinations on this list will be BLOCKED

ADDUPLOAD

CLEAR

www.cnn.com	DOMAIN	<i>Eg. CNN is hosting malware that is not on the blacklist</i>	
-------------	--------	--	--

Incident Response Blocking

Apply
Destination
list to
Roaming
Computers
Policy

Roaming Computers

Applied To
4 Identities

Contains
4 Policy Settings

Last Modified
Sep 20, 2017

Apply Destination Lists [ADD NEW LIST](#)

Search for and apply the appropriate block or allow Destination Lists for this policy. Click Add New List to create a Destination List.

Q Search...

☒

Showing: All Lists ▾ 3 Total

☒

Global Allow List

1 >

☒

Global Block List

0 >

☒

Roaming Computers Block List

1 >

1 Allow Lists Applied

☒

Global Allow List

1

2 Block Lists Applied

☒

Global Block List

0

☒

Roaming Computers Block List

1

[REMOVE ALL](#)

Incident Response Blocking

Use Policy Tester to Verify Results

Policy Tester

Test whether a destination will be allowed or blocked for an identity. If you receive results you don't expect or want, reorder or refine your policies and run the test again.

Identities

Ex: Roaming Computer, Network Devices, User, Site, Network, AD Group (max 1 of each)

🔒 nzaldiva-M-...

x

Destination

Note: Currently URLs are not supported

www.cnn.com

RESET

RUN TEST

Result:

🚫 **Destination was blocked due to a destination list**

Triggered Identity: nzaldiva-M-70SP

Destination: www.cnn.com

CNAMEs: turner-tls.map.fastly.net

Result: Destination was blocked due to a destination list

Destination List: Roaming Computers Block List

Categorization: News/Media, Business Services

Policy Applied: **Roaming Computers**

This identity was found in 2 policies. Out of these, **Roaming Computers** was the higher ranked policy, so it was applied to the identity. The other policy was your default policy, which is always your lowest ranked policy.

Note: Your actual results may differ from what's shown above if you have the Intelligent Proxy enabled, as URLs could be treated differently.



Am I by Protected by Umbrella?

<http://welcome.umbrella.com/>



Welcome to Umbrella!

Your internet is faster, more reliable and better protected because you're using Cisco Umbrella.

Intelligent Proxy -> <http://proxy.opendnstest.com>

With Decryption -> <https://ssl-proxy.opendnstest.com>

File Inspection -> <http://proxy.opendnstest.com/malicious.html>

Phishing testing - > <http://www.internetbadguys.com/>

Adult Content Testing -> <http://www.exampleadultsite.com>

<https://support.umbrella.com/hc/en-us/articles/115000411528-What-are-the-Umbrella-Test-Destinations->

Umbrella Provides Visibility

Identify Cloud services
being used (Shadow IT)
&
Integration with Cloudlock
for banned applications

Filtered by
Identity,
Service and
Date for
easy data
mining and
reporting

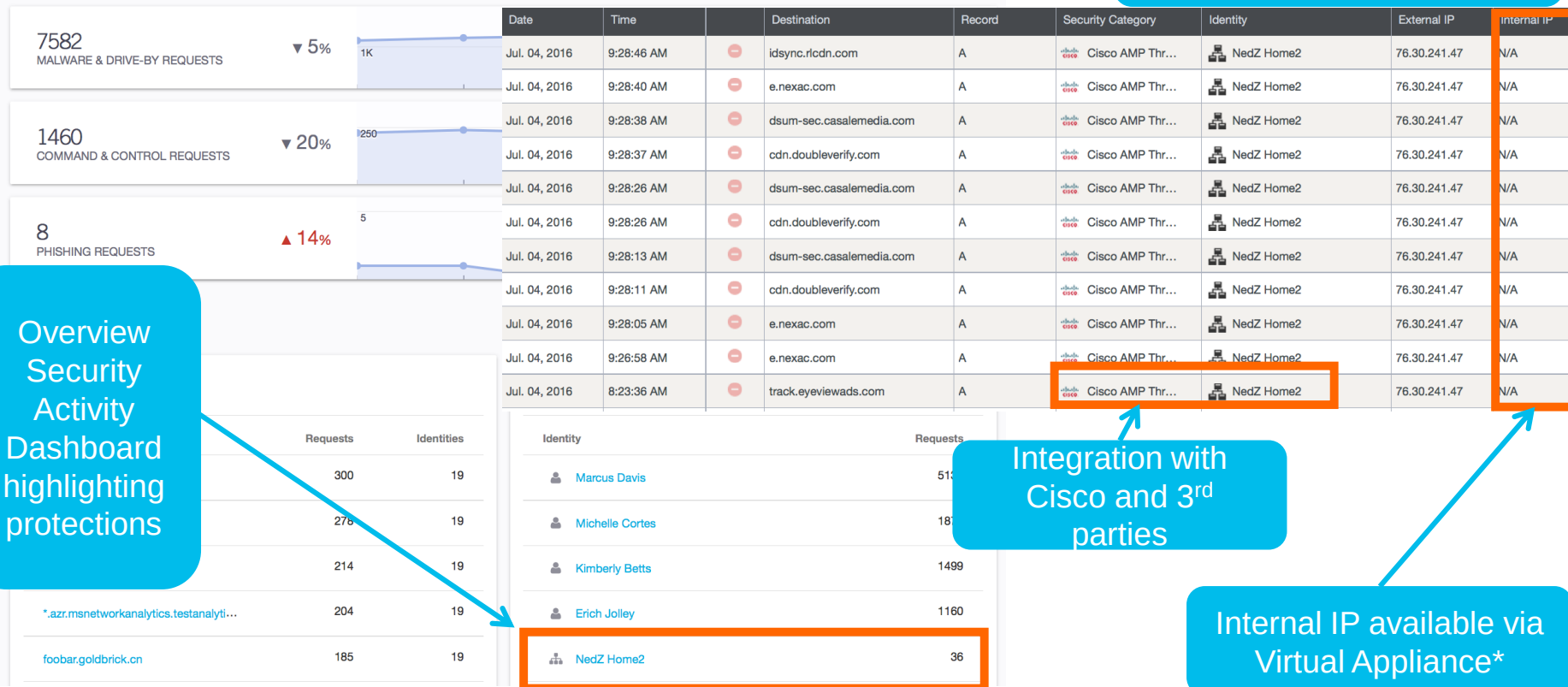
Activity Volume	12	0	3
Top Domains	Cloud Services	Never Before Seen	Total Identity Count
Top Categories			
Top Identities			
Exported Reports			
Scheduled Reports			
Admin Audit Log			

Name	Classification	Ident...	Trend	Req...	Bloc...	First ...	Last ...
Dropbox	File Sharing, Collab...	3	↓ 1	150	0%	Jun. 02, ...	Jul. 03, 2...
Cisco Webex	Web Conferencing, ...	1	↓ 3	63	0%	Jun. 02, ...	Jul. 03, 2...
Evernote	Business Managem...	2	↓ 2	57	0%	Jun. 02, ...	Jul. 03, 2...
Eye-Fi	Content Sharing	1	↓ 1	38	0%	Jun. 02, ...	Jul. 03, 2...
Box	Content Sharing, Fil...	1	↓ 1	17	0%	Jun. 02, ...	Jun. 30, ...
Zendesk	Customer Support, ...	1	↓ 2	4	0%	Jun. 02, ...	Jul. 01, 2...
Facebook	Social Media, Com...	1	↓ 2	3	0%	Jun. 02, ...	Jul. 01, 2...
OpenDNS Umbrella	Security	1	↓ 2	2	0%	Jun. 02, ...	Jul. 01, 2...
Oracle CRM On De...	CRM & SFA	1	↓ 1	2	0%	Jun. 03, ...	Jun. 30, ...
Google Analytics	Data & Analytics, Tr...	1	↓ 2	2	0%	Jun. 02, ...	Jul. 01, 2...

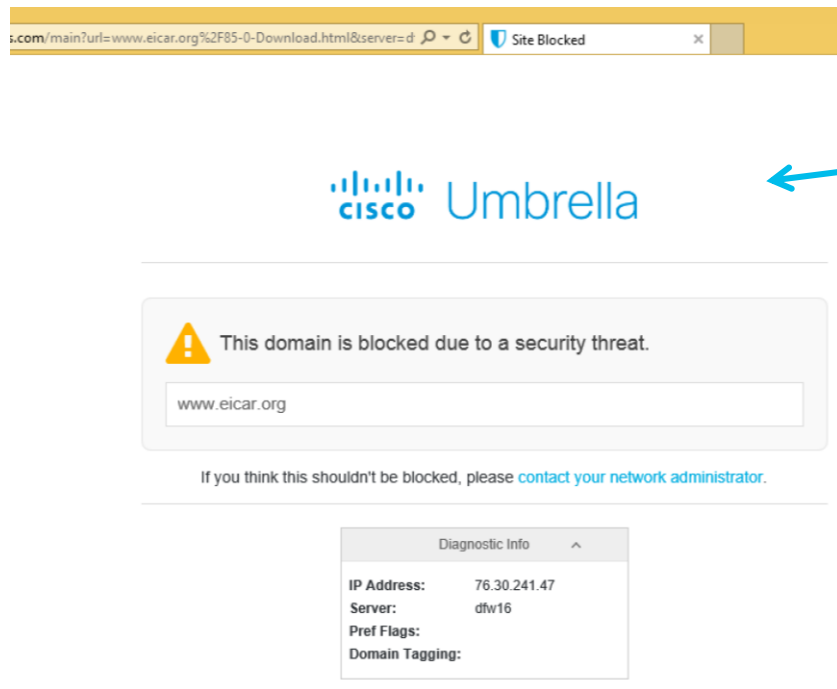
Find a Cloud Service	
Service Name:	<input type="text" value="Type a Cloud Service Name"/>
SHOW SERVICE DETAILS	
Filter Cloud Services	
Filter by Identity:	<input type="text" value="Ned's MacBook Pro"/>
Filter by date:	<input type="text" value="Last 7 Days"/>

Umbrella Provides Protection

Security Categories



Example of Blocking Malware from Being Downloaded



- By default Block pages are provided
- New Activity Search on:
 - DNS
 - Proxy
 - File

States of Client



Not Protected

Configuring



Roaming Security:

Checking connection state.
Please wait...

Unprotected



Roaming Security:

You are not currently protected by Umbrella.

Disabled



Roaming Security:

Disabled while you are on a trusted network.

Trusted Network

Protected

Protected/Encrypted – DNS over 443



Roaming Security:

You are protected by Umbrella.
DNS queries are encrypted.

Protected /Unencrypted – DNS over 53



Roaming Security:

You are protected by Umbrella.
DNS queries are not encrypted.

Protected



Roaming Security:

You are on a network protected by Umbrella.

By Network – Existing network is protected
By Virtual Appliance – provides Identity*

Admin

Offline



Roaming Security:

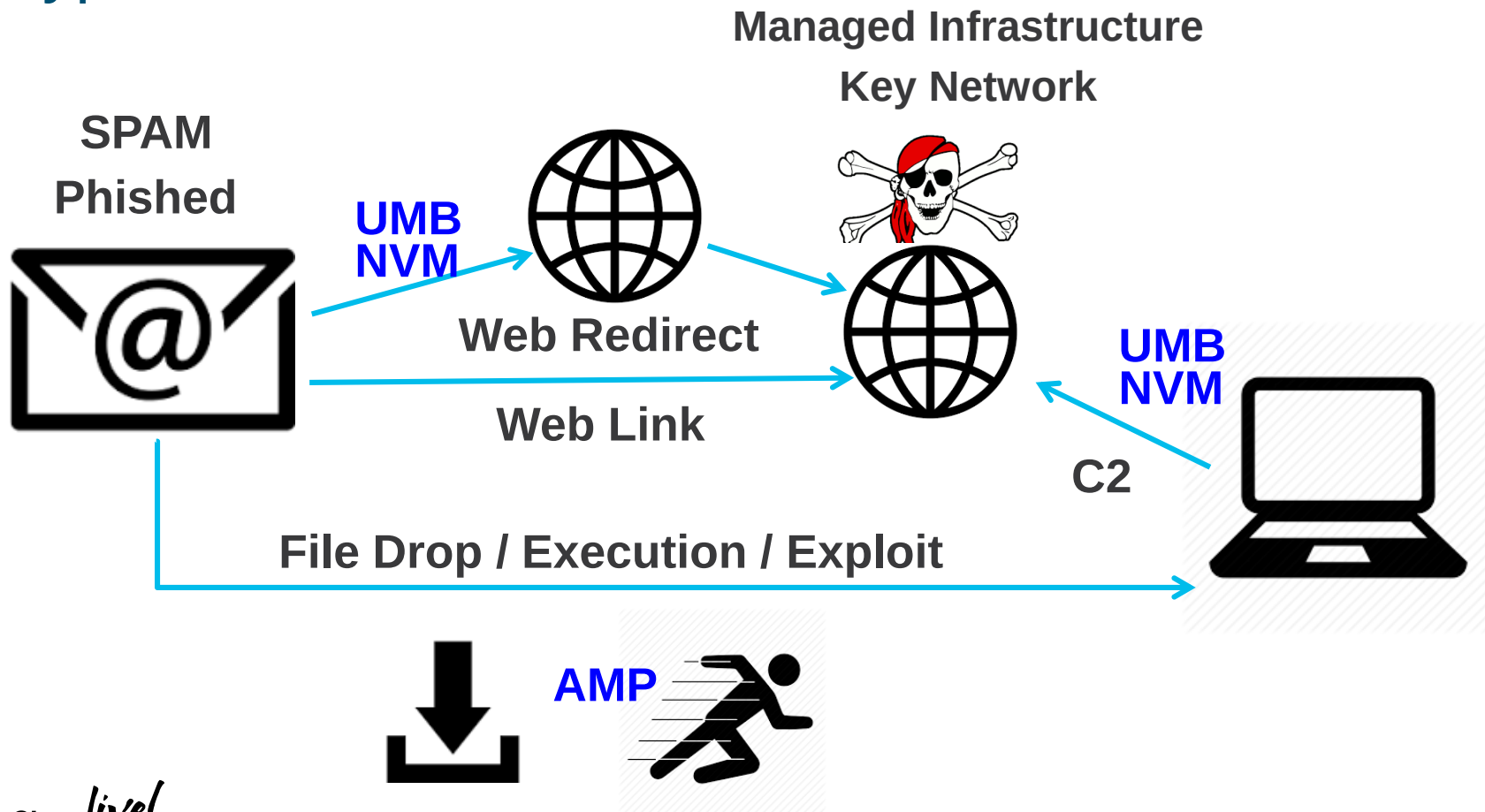
You are not currently protected by Umbrella.
Profile is missing.

Uninstalled

Umbrella Roaming Demo

Mapping to Threats

Typical Email Malware



Ransomware

Cerber

- Email
- Google Link
- Redirects to Tor2Web (no Tor client required)
- Malicious Word doc using Macros
- Call back to install
- Goal is to collect Ransom

CERBER RANSOMWARE - Instructions

CERBER RANSOMWARE

Instructions

English

Can't you find the necessary files?
Is the content of your files not readable?

It is normal because the files' names and the data in your files have been encrypted by "Cerber Ransomware".

It means your files are NOT damaged! Your files are modified only. This modification is reversible. From now it is not possible to use your files until they will be decrypted.

The only way to decrypt your files safely is to buy the special decryption software "Cerber Decryptor".

Any attempts to restore your files with the third-party software will be fatal for your files!

You can proceed with purchasing of the decryption software at your personal page:

<http://lfdachijzuwx4bc4.15rnwa.top/C7C3-E5AC-7FA0-0088-5324>

<http://lfdachijzuwx4bc4.dvalj9.top/C7C3-E5AC-7FA0-0088-5324>

<http://lfdachijzuwx4bc4.onion.to/C7C3-E5AC-7FA0-0088-5324>

Typical Web Malware

Compromised Web Site
Malvertising



**UMB
NVM**
Web Redirect



Managed Infrastructure
Key Network

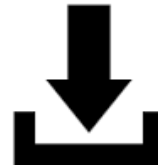


**UMB
NVM**
C2



File Drop /
Execution/
Exploit

AMP



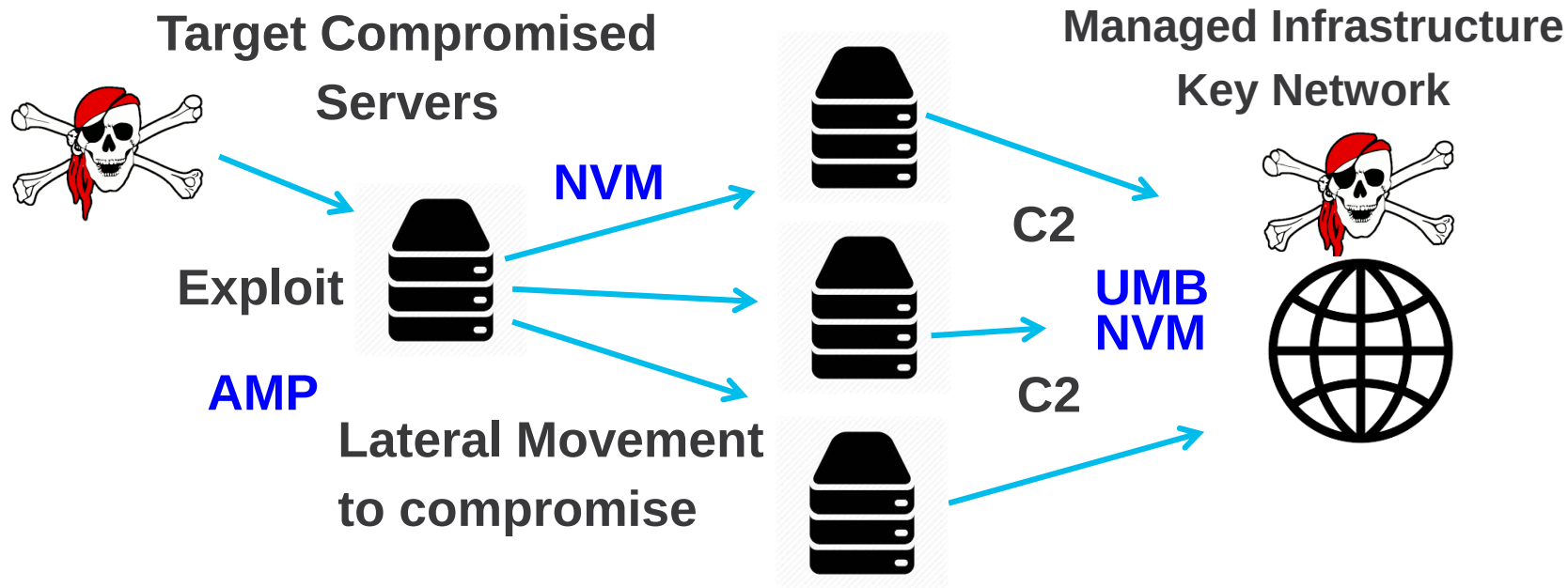
Malvertising

Kyle and Stan

- Using well known advertisers like winrar, amazon, and youtube
- Web Redirect
- Download what looks to be a legitimate tool
- Tool and malware is then installed.
- Goal to install on many Systems to bought or rented.



Targeted Malware



Targeted Ransomware

Sam Sam + variants

- Compromise servers using Jboss or other means
- Move lateral inside networks to other servers
- Infect with Ransomware
- Accept Bitcoin/Dollars...whatever

The screenshot shows a web browser window with a ransomware payment page. The page has a light blue header with a search bar. Below the header, there are two main sections: 'Your comments' and 'Our Answer'. The 'Your comments' section contains a text input field with the placeholder text 'comment here with your "Computer name" to receive decryption software.' and a button labeled 'Leave a comment'. The 'Our Answer' section contains two paragraphs of text. The first paragraph says 'Test decryption for [redacted] PC, check help, http://s000.ti/index.php?file_id=727012669578[redacted]'. The second paragraph says 'Sorry for delay, here you are: allKeys http://s000.tinyupload/index.php?file_id=50019761328[redacted]'. Below the 'Our Answer' section, there is a large light blue box with the text 'Leave a comment'.

Your comments	Our Answer
comment here with your "Computer name" to receive decryption software.	Test decryption for [redacted] PC, check help, http://s000.ti/index.php?file_id=727012669578[redacted]
[redacted] PC	Sorry for delay, here you are: allKeys http://s000.tinyupload/index.php?file_id=50019761328[redacted]
Leave a comment	

Endpoint Controls against Typical Malware



	Umbrella	Web Security	AMP4E	NVM	VPN - AlwaysON	Network Access Manager
Email	Rely on Centralised Controls, like Email Security Appliance	Rely on Centralised Controls, like Email Security Appliance	Rely on Centralised Controls, like Email Security Appliance	Rely on Centralised Controls, like Email Security Appliance	Rely on Centralised Controls, like Email Security Appliance	Rely on Centralised Controls, like Email Security Appliance
Web Link	Prevent with Intelligent Proxy - Grey	Prevent/Detect with Proxy	NA	Record Flow with URLs, Integration with Proxy	Rely on Centralised Controls	Rely on Centralised Controls
Web Redirect	Prevent with Intelligent Proxy - Grey	Prevent/Detect with Proxy	Device Flow Correlation/IP blacklist	Record Flow with URLs, Integration with Proxy	Rely on Centralised Controls	Rely on Centralised Controls
File Drop	Prevent with File Inspection (new)	Prevent/Detect with AV, AMP	Record, Simple Detection	Record / Flow with process name, Hash, Identity	Rely on Centralised Controls	Rely on Centralised Controls
File Execution	NA	Prevent/Detect with AV, AMP	Prevent/Record, Simple Detection	NA	Rely on Centralised Controls	Rely on Centralised Controls
Exploit Flash/PDF....	NA	Prevent/Detect with AV, AMP	Prevent/Record, Simple Detection	Record / Flow with process name, Hash, Identity	Rely on Centralised Controls	Rely on Centralised Controls
C2	Prevent/Detect with DNS Analytics	Prevent/Detect with Web Reputation,	Record, Device Flow Correlation/IP	Record / Flow with process name,	Rely on Centralised Controls	Rely on Centralised Controls

Endpoint Security Controls

Visibility, Prevention, Response



NVM – Endpoint using **Netflow/IPFIX**



Umbrella – **Network Blocking of Malware** using
DNS/IP and Intelligent Web Proxy



AMP4E – Used for **Incident Response** and
Prevention via Cloud Analytics/DB,
Exploit Protection and Antivirus



Other Endpoint Capabilities

See Appendix/Continue your education for details

- Posture
 - AnyConnect System Scan – ISE Posture
 - AnyConnect VPN Hostscan
- Device Management
 - Meraki Systems Manager
- Cisco Security Connector
 - BKSEC-3446 – Aaron Woland
- Troubleshooting
 - DART – Diagnostics and Reporting Tool

Anyconnect Secure Mobility Client

- Latest version is AnyConnect 4.4
- See table for OS Support



Anyconnect/AMP Platform/Modules



	Windows 7, 8.x, 10	Mac OSX	Linux	iOS	Android	Blackberry 10.3.2+	Win 8.1 Phone	ChromeOS 43+
VPN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Network Access Manager	Yes	No	No	No	No	No	No	No
Posture	Yes	Yes	Yes	No	No	No	No	No
Telemetry	Yes	Yes	No	No	No	No	No	No
Network Visibility	Yes	Yes	No	No	Yes, Samsung Knox	No	No	No
DART	Yes	Yes	Yes	No	No	Yes	Yes	Yes
Umbrella Roaming Security	Yes	Yes	No	Cisco Security Connector	No	No	No	No
AMP	Yes	Yes	Yes		Yes	No	No	No

AnyConnect Module Installation Options



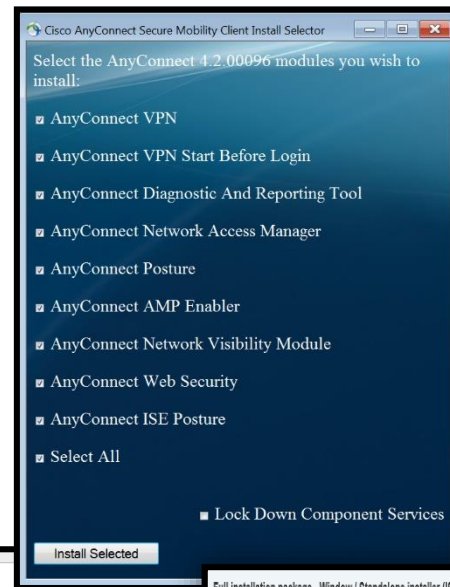
Package for your Favorite Deployment Tool



Mobile installed via App Store



Group Policy



Optional Client Modules to Download:

Always-On VPN:

Client Profiles to Download:

- ☒ AnyConnect DART
- ☐ AnyConnect AMP Enabler
- ☐ AnyConnect Network Visibility
- ☐ AnyConnect Posture
- ☐ AnyConnect Web Security
- ☐ AnyConnect OpenDNS
- ☐ AnyConnect ISE Posture

Full installation package - Window / Standalone installer (ISO), includes installer 23-DEC-2015
ion packages for DART, NAM, CoreVPN, Phone Home, Hostscan, ISE Posture, a
nd WebSecurity components.
anyconnect-win-4.2.01035-pre-deploy-k9.iso

27.07 MB



AnyConnect Module Installation Options



ISE Client Provisioning

ISE posture required for any module to be installed

AnyConnect Module Selection

ISE Posture ☒

VPN ☐

Web Security ☐

AMP Enabler ☐

Network Visibility ☒

ASA Posture ☐

Diagnostics and Reporting Tool ☐



Automatic Upgrades from
cisco.com if using Umbrella Roaming with
AnyConnect4.3*

* Can be disabled by some or all Users via VPN/ISE configuration

Summary

Endpoint provides:

- Un-encrypted views, Endpoint sees it all!
- Handles the Transitions to Cloud and Mobility
- **Prevention -> Visibility -> Response -> Control**

Ultimately the Endpoint, Needs same layers of defence your Network has!



Continuing your Education

SESSION ID	SESSION DESCRIPTION	SPEAKER
BRKSEC-2809	Deciphering TLS without Decryption – ETA / Joy	Blake Anderson
BRKSEC-2769	Endpoint Security – Cisco Security Connector / Meraki	Aaron Woland
BRKSEC-3014	Security Monitoring with Stealthwatch	Matt Robertson
BRKSEC-3230	A Deep Dive on How Threatgrid, AMP4E and Umbrella Integrate and Support IR	Eric Hulse / Dean De Beer
BRKSEC-1008	Simple Hacking Tools for Your Network	Jerry Lin
BRKSEC-2695	Buiding Enterprise Access Control (including Posture)	Jatin Sachdeva
BRKSEC-3053	Practical PKI with AnyConnect VPN	Ned Zaldivar
BRKSEC-2501	Deploying AnyConnect SSL VPN with ASA and FTD	Ned Zaldivar

Security Joins the Customer Connection Program

Customer User Group Program

- **Who can join:** Cisco customers, service providers, solution partners and training partners
- **Private online community** to connect with peers & Cisco's Security product teams
- Monthly **technical & roadmap briefings** via WebEx
- Opportunities to **influence product direction**
- Local **in-person meet ups** starting Fall 2016
- **New member thank you gift* & badge ribbon** when you join in the **Cisco Security booth**
- **Other CCP tracks:** Collaboration & Enterprise Networks



Join in World of Solutions

Security zone → Customer Connection stand

- Learn about CCP and Join
- New member thank-you gift*
- Customer Connection Member badge ribbon

Join Online

www.cisco.com/go/ccp

Come to Security zone to get your new member gift* and ribbon

Security Beta Programs

Security Customer Insights



Security Beta Products

ASA	Firepower NGFW/NGIPS	Firepower Platforms
AMP for Endpoints	ISR	ESA
ISE	Umbrella	

To participate in Beta:

<http://cs.co/security-beta-nomination>

or email

ask-sbg-beta@cisco.com

For Cisco Security Connector:

<https://cisco.com/go/apple/beta>



Customer Benefits

- Free test hardware
- Early experience with and training on new features and functionality
- Demos and feedback sessions on product usability, design, and roadmaps
- Risk-free testing in the customer environment prior to FCS
- Beta customer S1-3 issues fixed in GA release

"I've been involved in many beta programs ... I must say that this one has been the best organised. This beta has taken a very active, hands-on approach." -
Liberal Arts College Customer

Q & A

Complete Your Online Session Evaluation

- Give us your feedback and receive a **Cisco Live 2018 Cap** by completing the overall event evaluation and 5 session evaluations.
- All evaluations can be completed via the Cisco Live Mobile App.

Don't forget: Cisco Live sessions will be available for viewing on demand after the event at www.CiscoLive.com/Global.

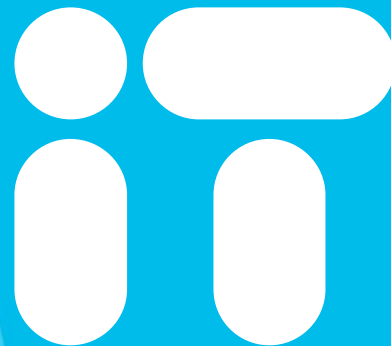




Thank you



You're



Cisco *live!*

Appendix/Bonus Materials

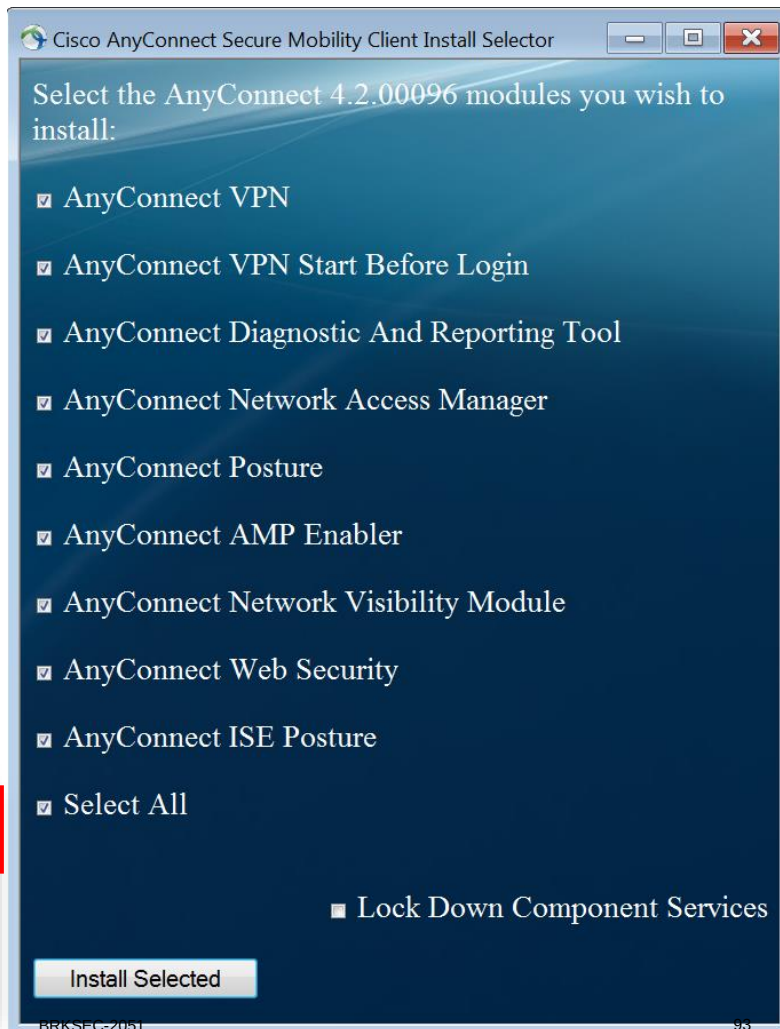
Anyconnect ISO Installation

- AnyConnect 4.3+ required for All Modules
- ASDM 7.6.1 or higher for All Modules
- ASA 9.2(1)+ for
 - ISE Posture over VPN
 - ISE Deployment of AC 4.x
 - CoA support
- ! Please check Anyconnect release notes!

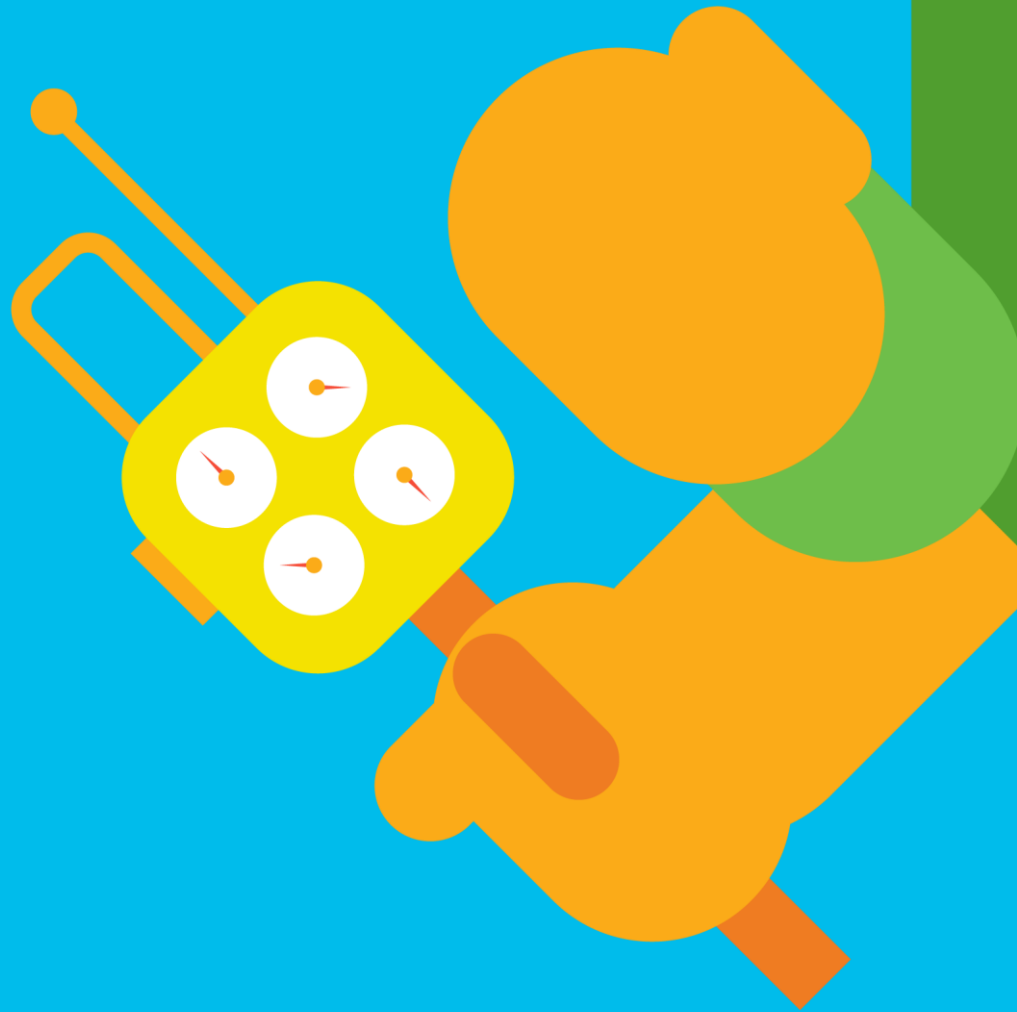
Full installation package - Window / Standalone installer (ISO). Includes installation packages for DART, NAM, Core/VPN, Phone Home, Hostscan, ISE Posture, and WebSecurity components.
anyconnect-win-4.2.01035-pre-deploy-k9.iso

23-DEC-2015

27.07 MB



DART (Troubleshooting)



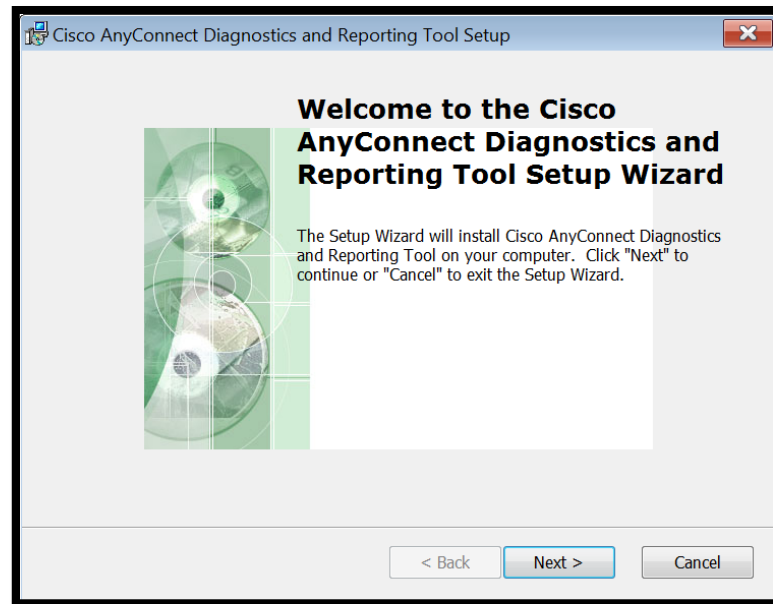
Diagnostics and Report Tool (DART)

Installation and Connection Troubleshooting

- End user must initiate for troubleshooting
- Zipped file saved on Desktop / Emailed (mobile)

TAC needs this troubleshoot!

- Connection or disconnection issues**
- Not passing traffic
- VPN service failure
- Software incompatibility
- Crashes, etc.



http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect42/b_AnyConnect_Administrator_Guide_4-2/troubleshoot-anyconnect.html#d42399e217a1635

What's Inside DART?



Name	Date modified	Type	Size
Cisco AnyConnect AMP Enabler Module	1/17/2016 11:45 A...	File folder	
Cisco AnyConnect ISE Posture Module	1/17/2016 11:45 A...	File folder	
Cisco AnyConnect Network Access Manager	1/17/2016 11:45 A...	File folder	
Cisco AnyConnect Network Visibility Module	1/17/2016 11:45 A...	File folder	
Cisco AnyConnect Posture Module	1/17/2016 11:45 A...	File folder	
Cisco AnyConnect Secure Mobility Client	1/17/2016 11:45 A...	File folder	
Cisco AnyConnect WebSecurity Module	1/17/2016 11:45 A...	File folder	
General Information	1/17/2016 11:45 A...	File folder	
summary	1/17/2016 11:43 A...	Text Document	41 KB

- NetworkVisibility
- NVM
- NVM_ServiceProfile

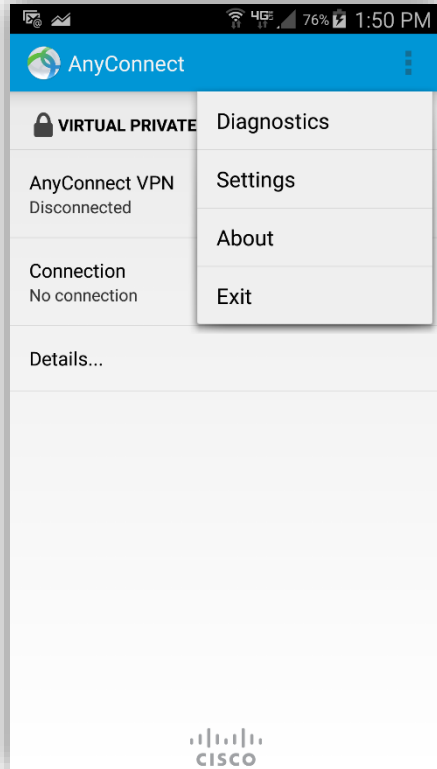
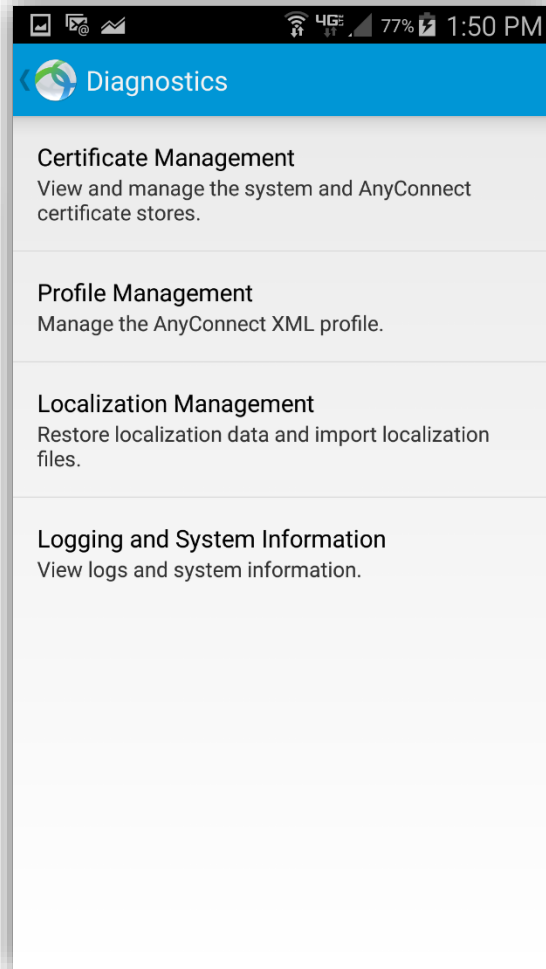
- 2.0_VPN
- acvpn
- Alpha_VPN
- AnyConnect
- AnyConnect
- AnyConnect_pre3.0
- AnyConnectLocalPolicy
- AnyConnectProfile.xsd
- anyconnect-win-4.2.01014-web-deploy-k...
- hosts
- OnConnect_AnyConnect_Screenlock_v2
- preferences
- preferences_global
- setupapi.app
- setupapi.dev
- UIHistory_20160117_093543_log
- update
- update_pre3.0
- UpdateHistory_20160117_091713_log

- WebSecurity.config
- WebSecurity
- WebSecurity
- WebSecurity_config.backup
- WebSecurity_ServiceProfile.wso
- WebSecurityCert.cfg

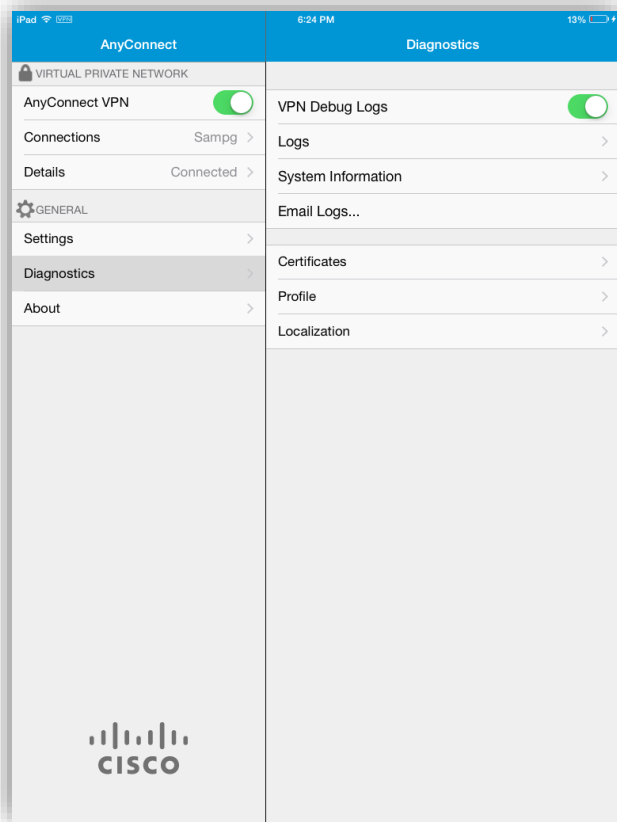
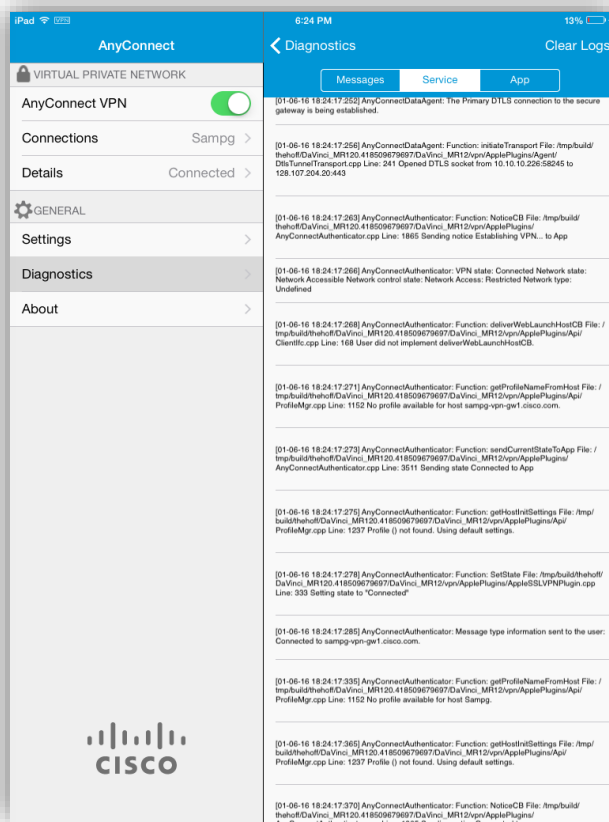
- AMPEnabler
- AMPEnabler
- AMPEnabler_ServiceProfile
- PersistedData.dat

- aciseposture
- AnyConnect_ISEPosture
- AnyConnect_ISEPosture
- ConnectionData
- ISEPostureCFG

Android Diagnostics

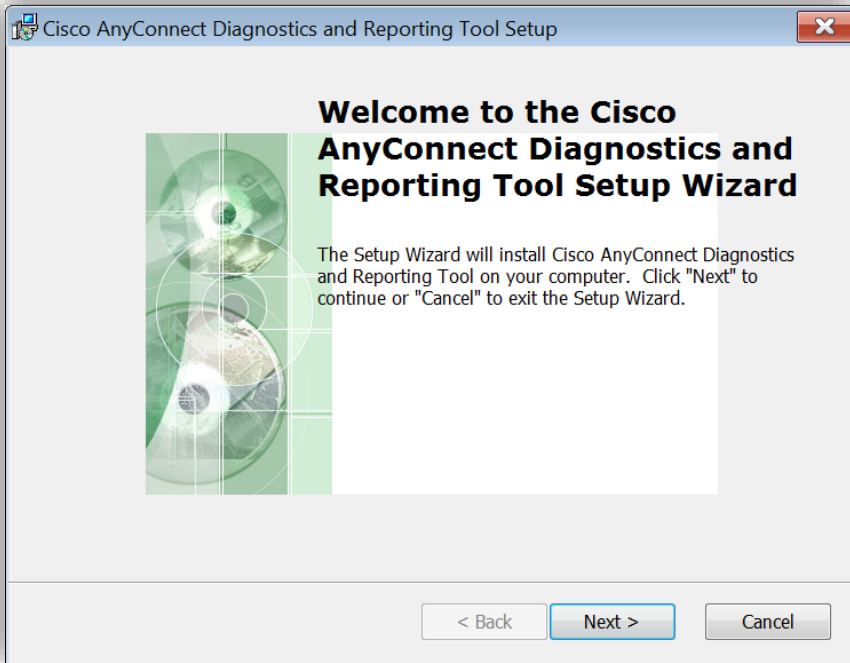
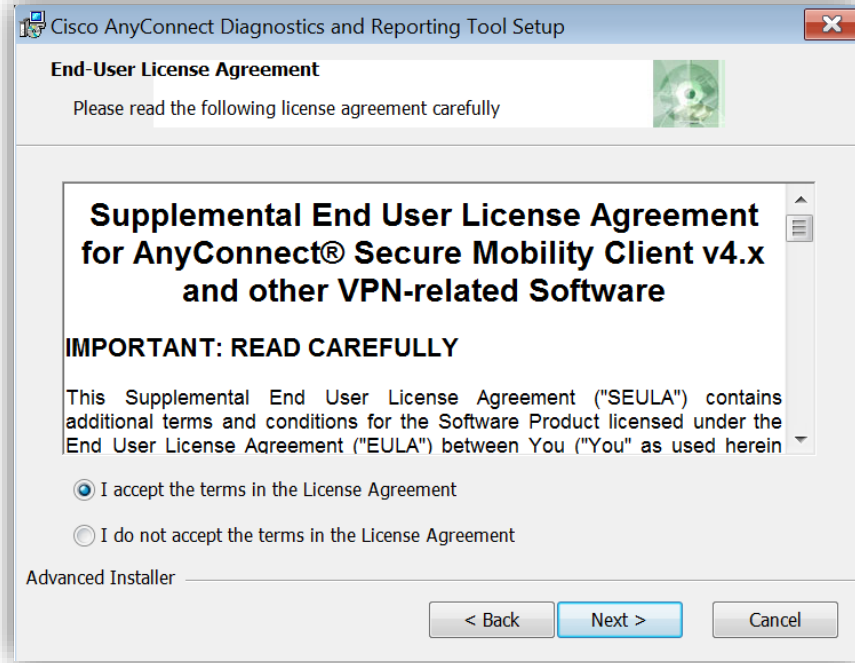


iOS Diagnostics



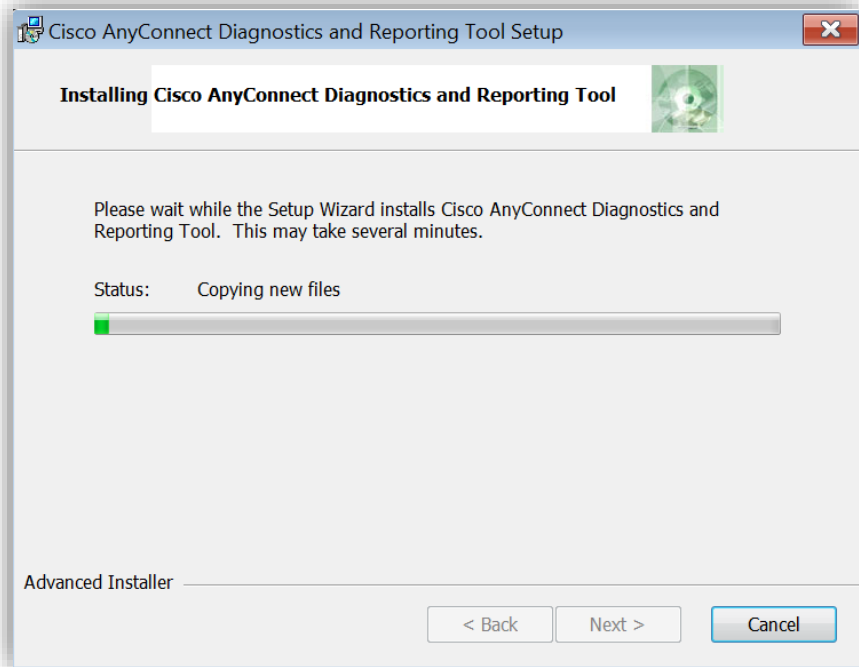
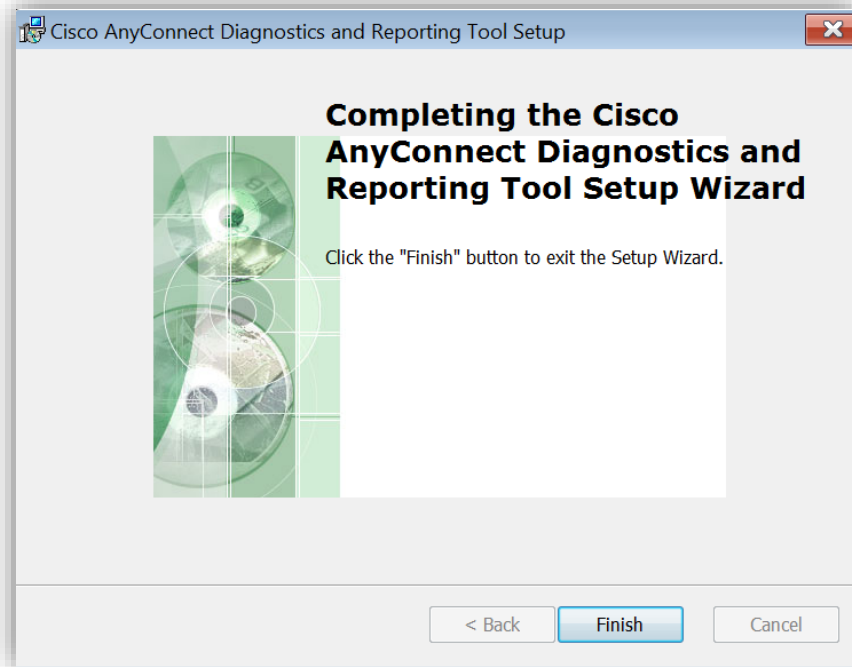
DART

Installation



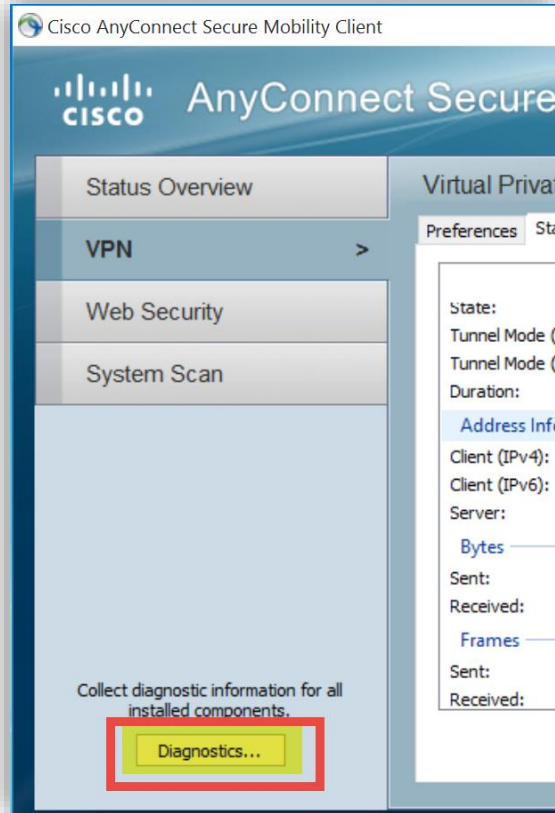
DART

Installation



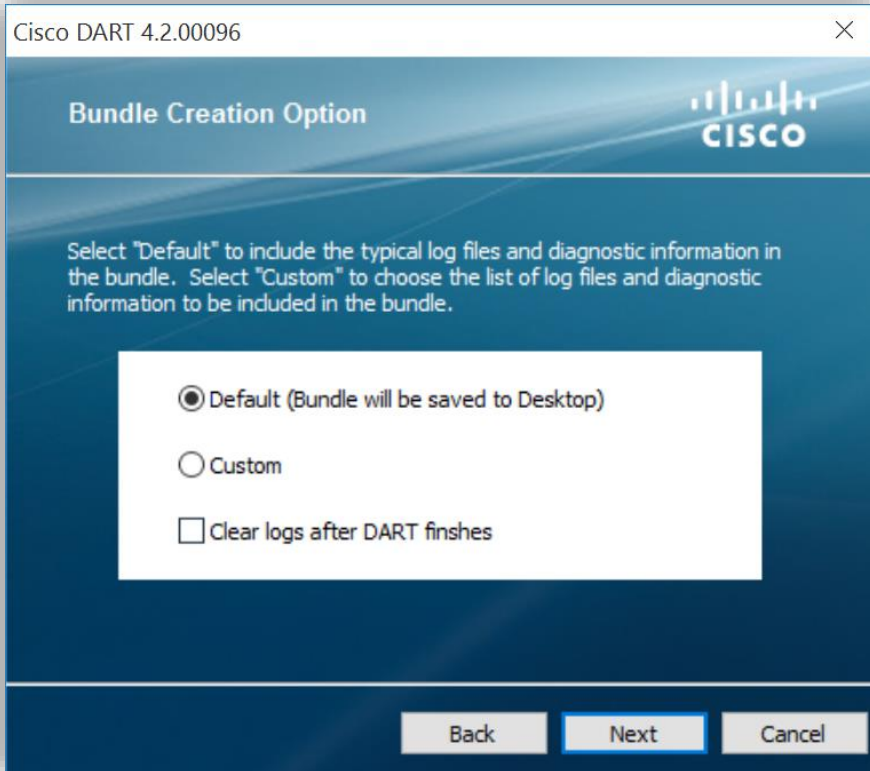
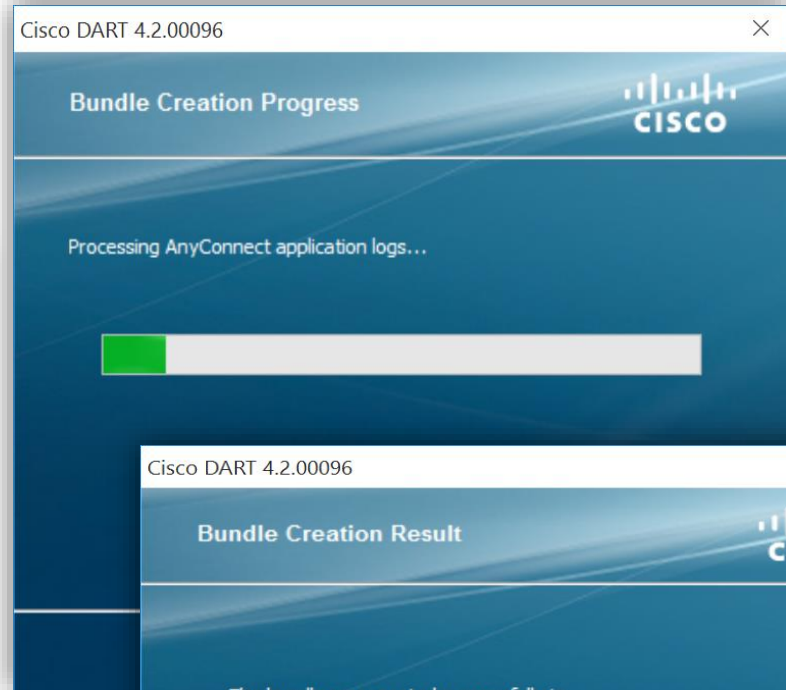
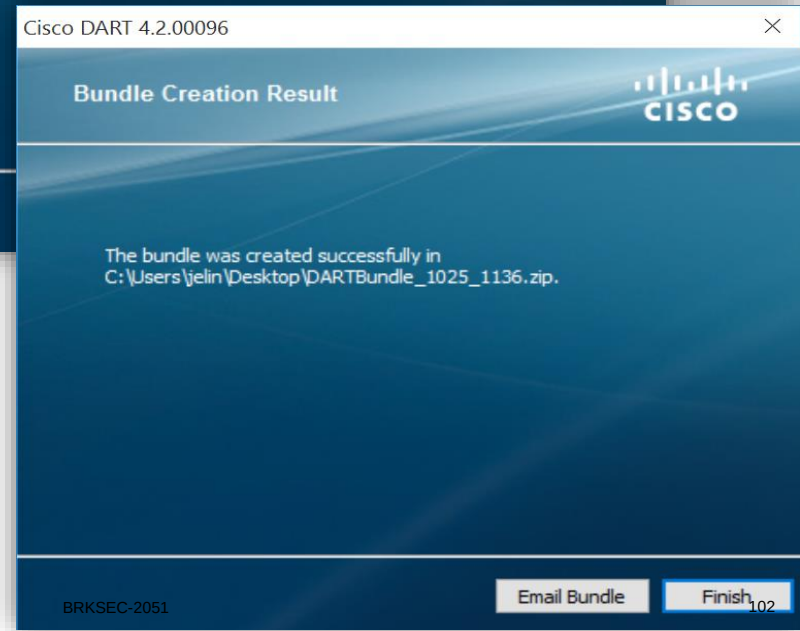
DART

For Troubleshooting



DART

For Troubleshooting



DART Customer Story

ASA 5555 - Troubleshooting Assistance

Summary

Notes

Attachments

Actions

From	Title	Created
▼ Marlon [REDACTED] ...	Resolution Summary	16-NOV-2015 09:35:45..
	I verified the ASA configuration and the DART logs We confirmed the configuration is OK and that the logs show there is a connectivity issue I explained that this is an external factor out of our control The customer understood and authorized to close the case.	
▼ Marlon [REDACTED] ...	KT Action Plan	16-NOV-2015 08:53:00..
	1. Contact Customer 2. Initiate a WebEx session 3. Verify webvpn, tunnel-group and group-policy config 4. Check DART logs 5. Provide a solution to the case	

Date : 10/29/2015

Time : 09:29:10

Type : Error

Source : acvpnagent

Description : Function: CSocketTransport::OnTimerExpired

File: .\IPC\SocketTransport.cpp

Date : 10/29/2015

Time : 09:29:10

Type : Warning

Source : acvpnagent

Description : Function: CNetEnvironment::logProbeFailure

File: .
etEnvironment.cpp

Line: 1431

Invoked Function: CHttpProbeAsync::SendProbe

Return Code: -27066354 (0xFE63000E)

Description: HTTP_PROBE_ASYNC_ERROR_CANNOT_CONNECT

HTTPS (host: [REDACTED] 25.1)

Date : 10/29/2015

Time : 09:29:10

Type : Warning

Source : acvpnagent

Description : Function: CNetEnvironment::TestAccessToSG

File: .
etEnvironment.cpp

Line: 1292

Invoked Function: CNetEnvironment::analyzeHttpResponse

Return Code: -28966899 (0xFE46000D)

Description: NETENVIRONMENT_ERROR_PROBE_INCOMPLETE:Network Probe could not contact target

These indicate a temporary connectivity issue between the client computer and the ASA. Please verify the connectivity if the disconnect happens again. I hope this helps you.

DART Module

Pros



- All details can be gathered when there is a problem
- Invisible to end user

Cons



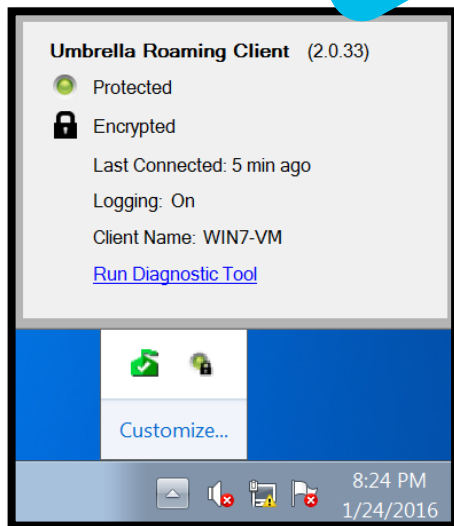
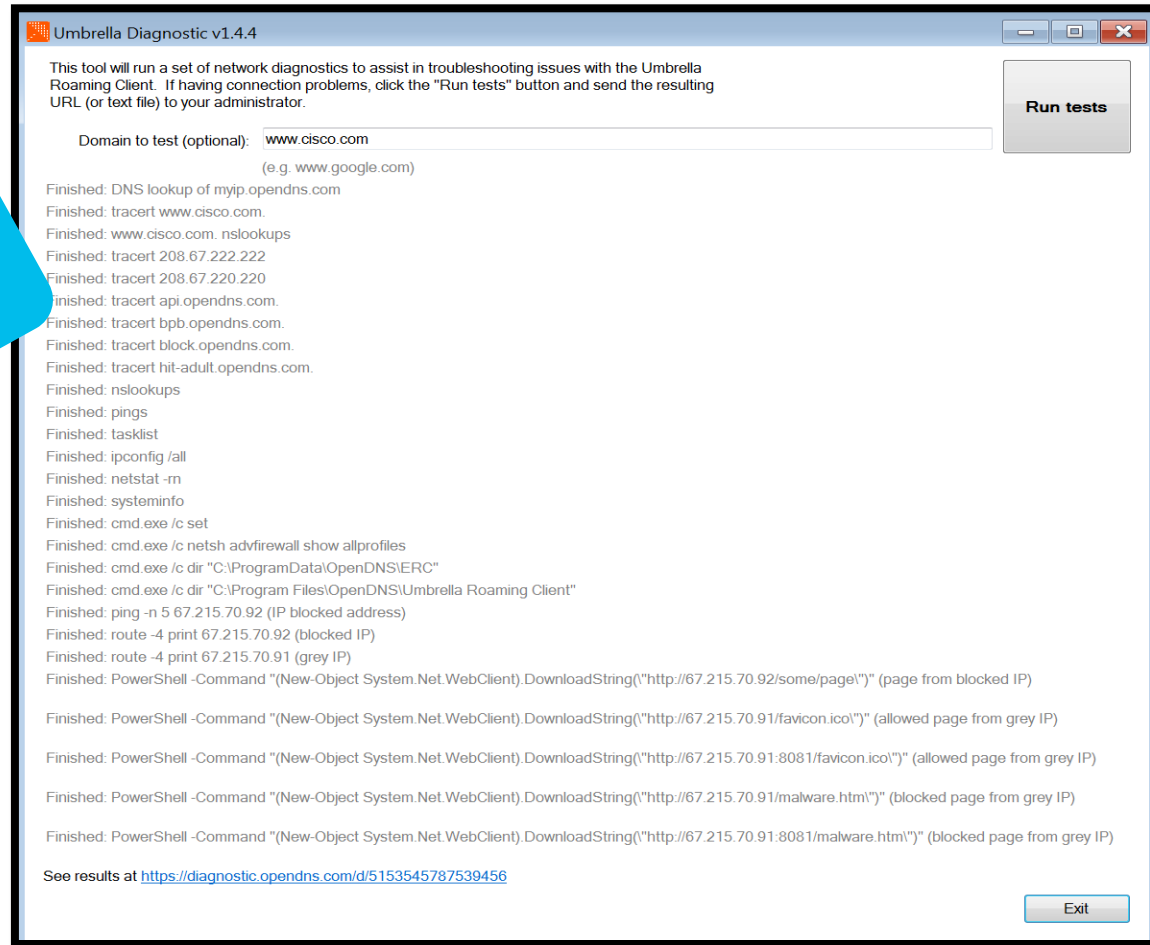
- Requires end-user to trigger
- Requires TAC to decipher



More Details on Umbrella

Roaming Client for PC

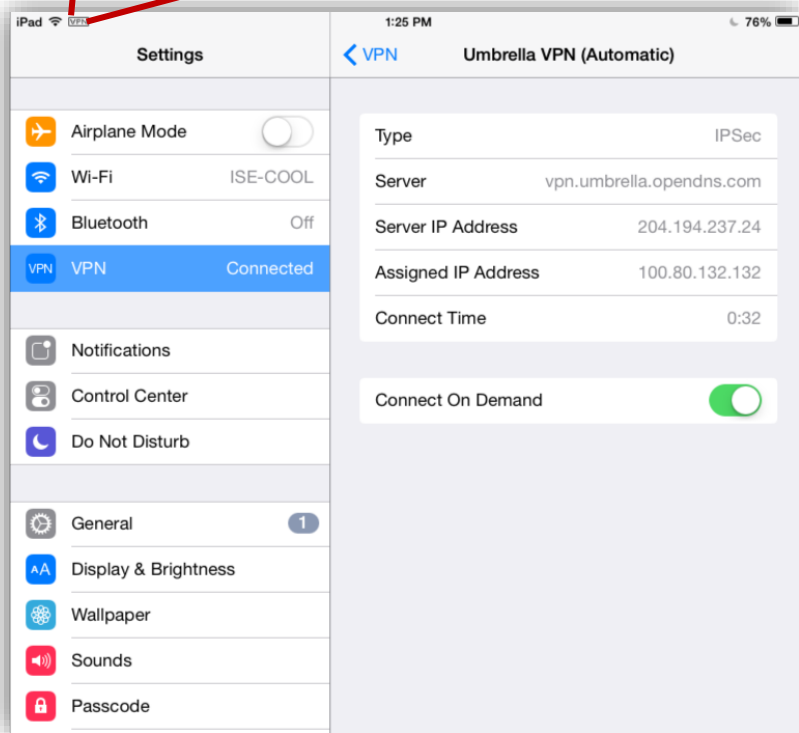
Major Difference:
Can be hidden
from end user



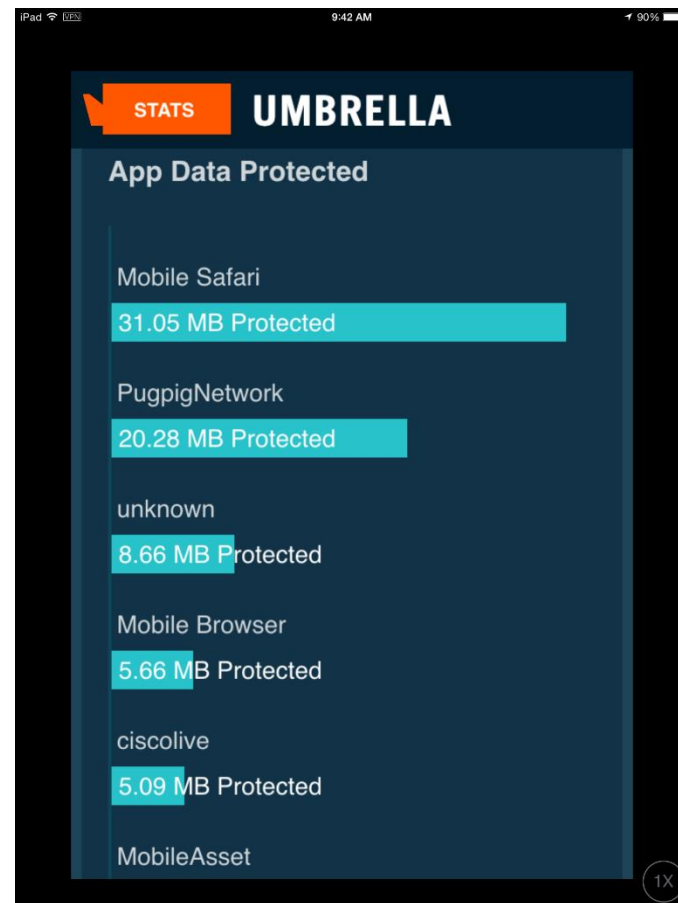
Umbrella for iOS (Still being Maintained, but not Option for New Customers)

VPN

VPN Required because only way to update DNS on across platform



Cisco *live!*





Roaming Security for iOS

PROTECT YOUR IOS DEVICE

- 1 Download our mobile app →
- 2 Customize your policy →
- 3 View reports

Download our mobile app

Install Umbrella for Mobile on your iOS device to protect your iPhone or iPad from phishing, malware, and more, no matter where you're connecting to the Internet.

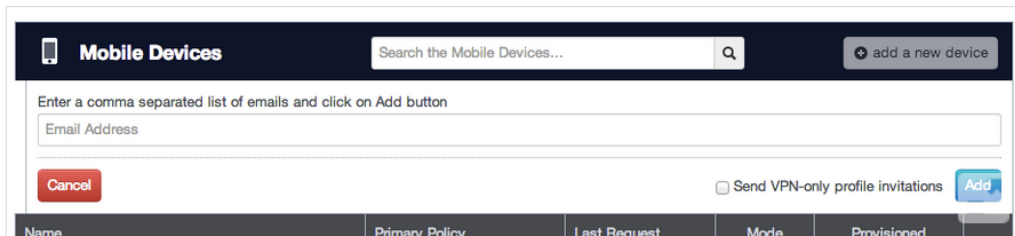
For a full guide to installing & configuring mobile devices, refer to the [Mobile Device Provisioning & Setup Guide](#) .

Roaming Security for iOS



Step 1 - Email an invitation to your mobile device

In the dashboard, go to [Configuration -> Identities -> Mobile Devices](#)  and select "add a new device."



Name	Primary Policy	Last Request	Mode	Provisioned
------	----------------	--------------	------	-------------

Enter an email address that you can access from the mobile device, then check to see if you've received an email from 'umbrella@opendns.com'.

Step 2 - Install and Activate your Umbrella for Mobile protection

Follow the instructions in the email to install Umbrella for Mobile. Click the link to download our app from the App Store; then return to the email and click the activate button.

Once activated, a VPN icon will appear in the status bar at the top of the screen.

Step 3 - Verify your device in the Dashboard

Return to [Configuration -> Identities -> Mobile Devices](#) , and check to see the device listed.



Roaming Security for iOS

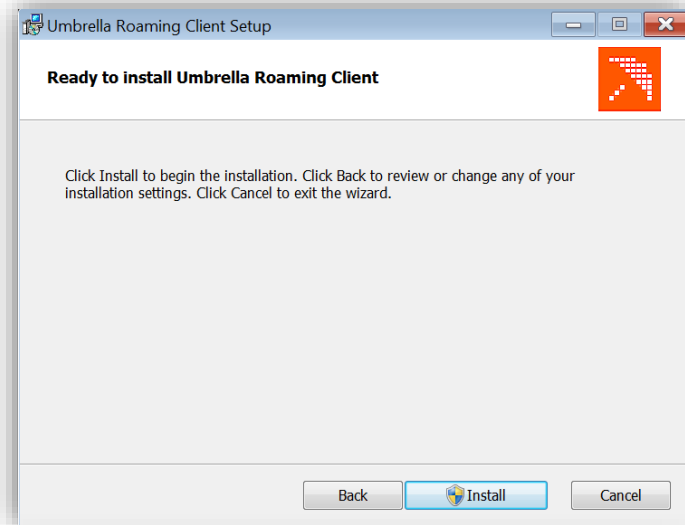
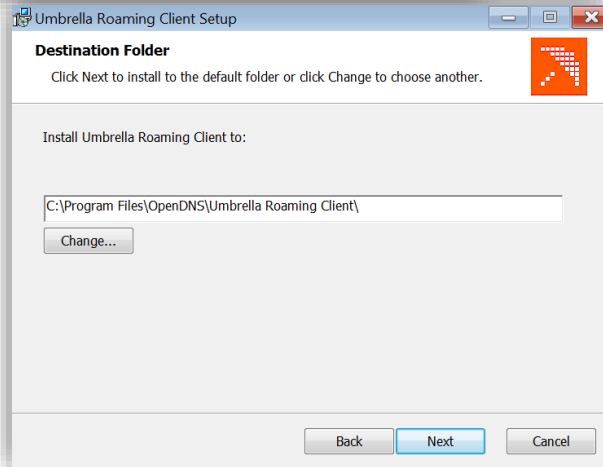
 SETUP GUIDE  OVERVIEW  CONFIGURATION  REPORTS

Warning: Upgrading to iOS 8 after deploying any VPN like Umbrella Mobile will cause connectivity issues. Please [read this article](#) on how to avoid these issues. 

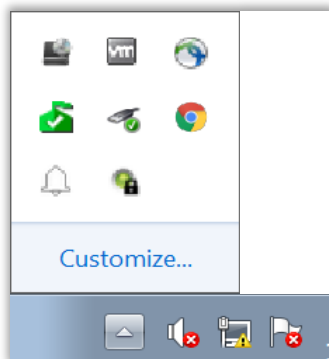
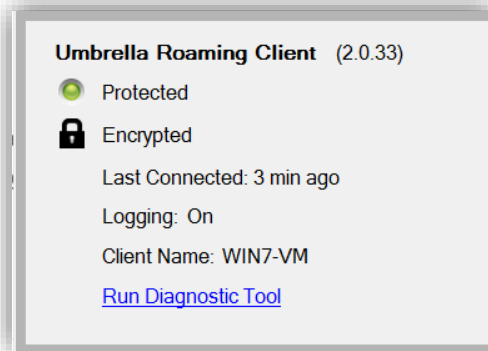
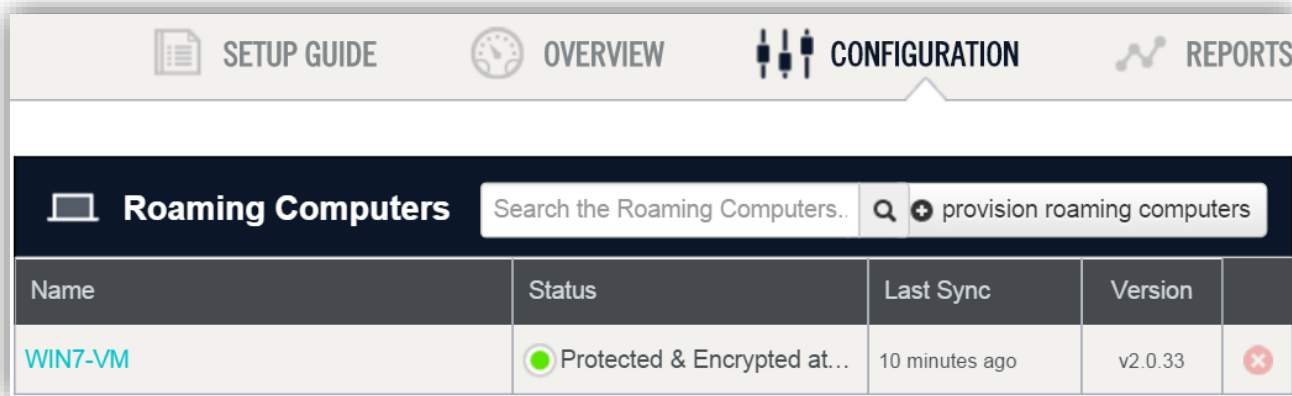
 **Mobile Devices**   add a new device

Name	Primary Policy	Last Request	Mode	Provisioned	
Jerry's iPad	Default Policy	a few seconds ago	 + 		

Windows Install - Roaming



Windows Install – Roaming Security



Umbrella Roaming:

Pros



- Increased Protection from Malware like Ransomware, Phishing, C2 callbacks and other threats
- Very Lightweight
- Essentially invisible security
- Can be deployed standalone
- Investigation add-on Engine for further details on domain/url

Cons



- Only visibility based on ingress/egress to client.



Cisco on Cisco Case Study

<http://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/m-sec-06292016-openDNS.html>

Details on Posture

Endpoint Posture:

Pros



- Provides policy to ensure endpoint is hardened
- Agent can quarantine if non-compliant
- Provides Visibility on the endpoint on what you are checking for

Cons



- Policy is more complex!
- User Experience changes
- Higher level of Support required



Cisco on Cisco Case Study

http://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/ISE_Cisco_on_Cisco_Trends_in_IT.html



ISE Posture using ISE:

File – Date, Exists, CRC32, SHA256

Registry – Windows Only

Application – process running

Service – service running

Regular Compound – Combine

Anti-Virus – Installed, Updated

Anti-Spyware – Installed, Updated

Patch Management – New for 2.0,
Installed, Enabled, Up to Date

Disk Encryption – New for 2.0, State

USB Detection – New for 2.1



ASA Hostscan using Dynamic Access Policies

Anti-Spyware – Version, Installed, Scanning Enabled, Last Update

Anti-Virus - Version, Installed, Scanning Enabled, Last Update

Application – AnyConnect, ikev1, Cut-thru, Ikev2

AnyConnect / System Attributes – OS, AnyConnect Version, Platform, Device ID

File – Existence, Age, CRC32 check

Device Attributes – Listening port numbers, Mac Address, Hostname

Operating System

Personal Firewall – Installed, Enabled, Version

Policy – prelogin assessment (not available)

Process – running on system

Registry – eg. Joined to Domain

Automated Remediation Possible for Personal Firewall, Anti-Virus and Anti-Spyware



ASA Hostscan Configuration

- Installed from ASA, File downloaded from Cisco.com
- Can be enabled/disabled on a per Connection profile

Configuration > Remote Access VPN > Host Scan Image

Use this panel to install Host Scan. The Host Scan image can come from a stand-alone package, or included as part of the AnyConnect 3.0 and 3.1 for Windows OS or the Cisco Secure Desktop packages.

Host Scan configuration can be performed by going to Secure Desktop Manager/Host Scan. If 'Host Scan' is not visible under 'Secure Desktop Manager', you will need to restart ASDM.

Location:

☒ Enable Host Scan/CSD

CSD/Pre-Login Gone!

• Hostscan images



ASA Hostscan

- Remediation possible for **Personal Firewall**, Anti-Virus and Anti-Spyware.

Personal Firewall

Vendor	Product	Note
Microsoft Corp.	Microsoft Windows Firewall 8	Supports firewall rules

Firewall Action: **Force Enable** ▼

Rules

Add... Edit... Delete

The action and rules remain effective on client device even after VPN session ends, please use them with discretion.



VPN Best Practices Deployment Options

- AnyConnect client deployed via MSI with SCCM or similar tools
- MDM deployment is also used for smartphones
- 2 forms of authentication used
 - Token + AD Username/Password
 - Certificate + Username/Password
- Usually deployed with ACS or ISE for logging (passed and failed AuthC)
- Smaller customers just leverage AD directly for user authentication/authorisation
- Full Tunnel mode with Local Lan access for printers
- Posture with ISE for centralised controls

ISE Posture Configuration

- Client Provisioning via ISE, requires AnyConnect Profile and Configuration

Remediation timer	4 mins
IP Address Change	
Parameter	Value
Enable agent IP refresh	Yes
VLAN detection interval	0 secs
Ping or ARP	Ping
Maximum timeout for ping	1 secs
DHCP renew delay	1 secs



AnyConnect Configuration > AnyConnect Configuration

* Select AnyConnect Package: AnyConnectDesktopOSX 4.2.96.0

* Configuration Name: AnyConnect ISE Posture and NVM

Description:

Description Value

* Compliance Module: AnyConnectComplianceModuleOSX 3.6.10255.2

AnyConnect Module Selection

- ISE Posture ☒
- VPN ☐
- Web Security ☐
- AMP Enabler ☐
- Network Visibility ☒
- ASA Posture ☐
- Diagnostic and Reporting Tool ☐

Profile Selection

- * ISE Posture: AnyConnect ISE Posture
- VPN
- Web Security
- AMP Enabler
- Network Visibility: NVM
- Customer Feedback

Other modules can be added

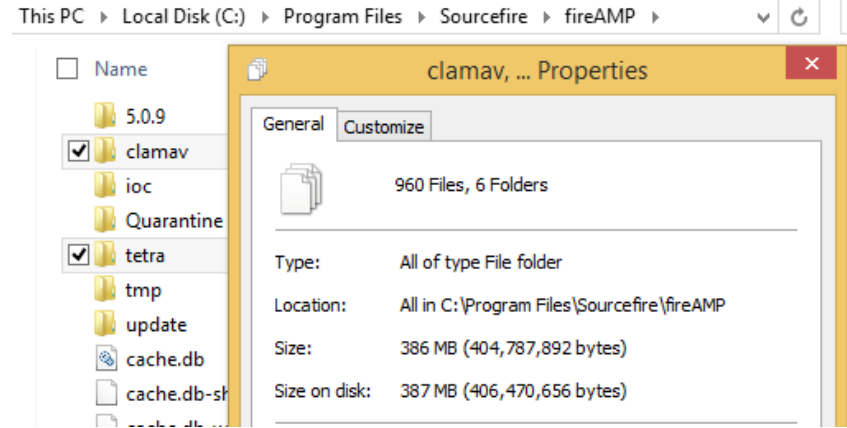


mac_posture_nvm	If	Any	and	Mac OSX	and	Condition(s)	then	AnyConnect ISE Posture and NVM
-----------------	----	-----	-----	---------	-----	--------------	------	--------------------------------

Details AMP4E

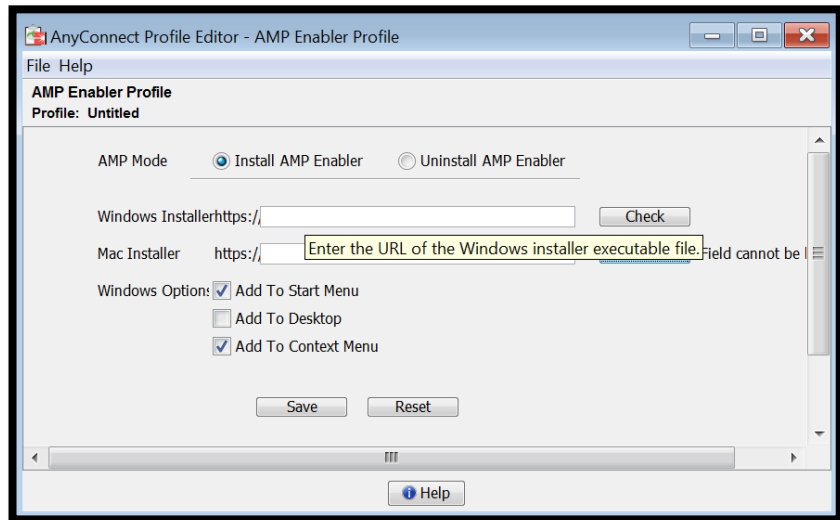
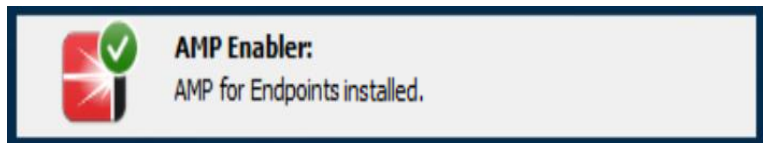
Install Details

- Initial install File is ~40MB
- ~390MB for clamAV and Tetra
- Total is around ~615MB
- Program Files > Sourcefire > fireAMP
- Tetra Updates every 24 hours by default



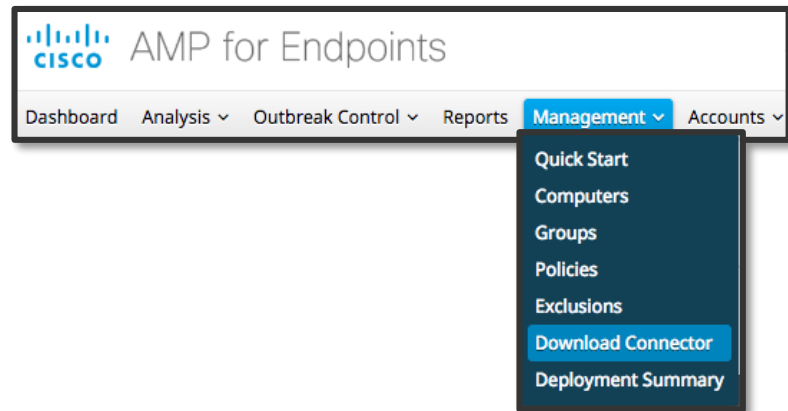
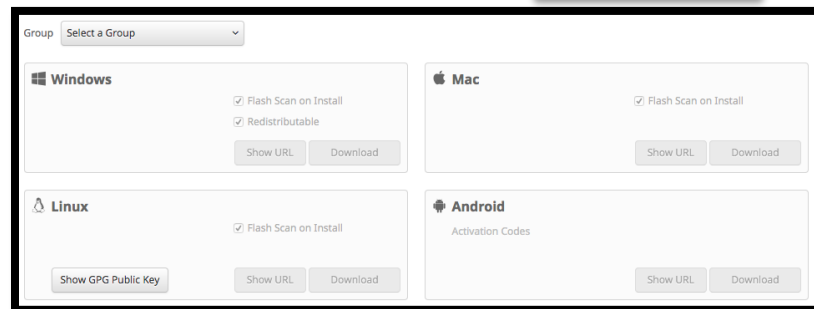
AMP4E Deployment Through ISE or ASA or Directly from Portal

AMP Enabler Profile Editor



Cisco *live!*

Direct from Portal / Via URL



AMP4E :

Pros



- Full Visibility & Control files execution
- No need to wait for a signature, admin has full control
- Provides prevention/detection for both on and off network
- Cloud managed, no upgrade
- Integrated with AMP for Networks, IoC, OpenIoC
- Can be deployed as standalone

Cisco *live!*

Cons



- Deployment Integration with AnyConnect only



Cisco on Cisco Case Study

<http://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/itb-sec-04252015-amp-for-everywhere.html?cachemode=refresh>

AMP4E - Quarantine

Event Type: Quarantine

Endpoint Logs

Results returned: 57

Date	Event	Details
7/6/15, 1:38:45 PM	Quarantine	/Users/nedzaldivar/Downloads/5c295d8d6675f4de964bef6076bb29b05cd6824760eda9ca5264f1f1838205c6.bin - W32.5C295D8D66-100.SBX.TG
7/6/15, 1:11:06 PM	Quarantine	/Users/nedzaldivar/Downloads/ee37ad9874316b8120a105827fb40e120abb87211cba172f27a6e83155709fef.bin - W32.Variant:Reputation.18fy.1201
6/26/15, 4:57:59 PM	Quarantine	/Users/nedzaldivar/Downloads/Zombies.pdf - W32.Zombies.NotAVirus
6/26/15, 4:56:45 PM	Quarantine	/Users/nedzaldivar/Library/Caches/com.apple.Safari/fsCachedData/OF5A21DB-106D-48CE-B545-A128C111C776 - W32.Zombies.NotAVirus
6/26/15, 4:54:41 PM	Quarantine	/Users/nedzaldivar/.Trash/eicarcom2.zip - W32.EICAR.16g1
6/26/15, 4:54:41 PM	Quarantine	/Users/nedzaldivar/.Trash/eicar_com 16-43-26-291.zip - W32.EICAR.16g1
6/26/15, 4:54:41 PM	Quarantine	/Users/nedzaldivar/Downloads/eicar-3.com - EICAR:EICAR_Test_file_not_a_virus-tpd
6/26/15, 4:54:41 PM	Quarantine	/Users/nedzaldivar/Downloads/eicar-4.com - EICAR:EICAR_Test_file_not_a_virus-tpd

12/11/15, 9:27:17 AM	Quarantine	/Users/nedzaldivar/Downloads/z.exe - GenericKDV:VBCrypt-tpd			
12/10/15, 1:44:48 PM	Quarantine	/Users/nedzaldivar/Library/Caches/Firefox/Profiles/0w2eiaan.default-1390923714428/cache2/entries/223F3C9942801939AE737F52B4DDA758E53B9FF2 - Swf.Exploit.CVE_2015_3102			
12/5/15, 1:49:35 PM	Quarantine	/Users/nedzaldivar/Library/Caches/Firefox/Profiles/0w2eiaan.default-1390923714428/cache2/entries/223F3C9942801939AE737F52B4DDA758E53B9FF2 - Swf.Exploit.CVE_2015_3102			
11/29/15, 10:22:52 AM	Quarantine	/Users/nedzaldivar/Library/Caches/Firefox/Profiles/0w2eiaan.default-1390923714428/cache2/entries/223F3C9942801939AE737F52B4DDA758E53B9FF2 - Swf.Exploit.CVE_2015_3102			
11/29/15, 10:19:06 AM	Quarantine	/Users/nedzaldivar/Library/Caches/Firefox/Profiles/0w2eiaan.default-1390923714428/cache2/entries/223F3C9942801939AE737F52B4DDA758E53B9FF2 - Swf.Exploit.CVE_2015_3102			
10/26/15, 7:22:54 AM	Quarantine	/Users/nedzaldivar/Library/Caches/Firefox/Profiles/0w2eiaan.default-1390923714428/cache2/entries/F00F15772E41F7EEDCEA38565D0621A817046ED0 - Swf.Exploit.CVE_2015_3102			
10/19/15, 11:34:34 AM	Quarantine	/Volumes/504/Windows/pwdump6-1.6.0.zip - W32.PWDump			
10/19/15, 11:34:22 AM	Quarantine	/Volumes/504/Windows/pwdump3.zip - Application:Hacktool-tpd			
10/19/15, 11:34:22 AM	Quarantine	/Volumes/504/Windows/ca_setup_4.9.43.exe - W32.Application:PUPGen.18lj.1201			

Endpoint IoC Example – W32.Locky.ioc (XML Format)

--Snipped

```
<IndicatorItem id="f652b38a-5550-474b-b664-762bdad04cc9"  
condition="contains">
```

```
<Context document="FileItem" search="FileItem/FileName" type="mir" />
```

```
<Content type="string">_Locky_recover_instructions.txt</Content>  
</IndicatorItem>
```



AMP4E Deployment Tips

- Follow the TechZone link for exclusions which should be in from the beginning. <http://www.cisco.com/c/en/us/support/docs/security/sourcefire-fireamp-endpoints/118341-configure-fireamp-00.html>
- Work with your AMP team to find custom exclusions for your environment
- Create multiple groups, instead of monolithic policies
- Use small groups to test deployment changes before implementing them.
- Leave the maximum scan size at 10MB
- ONLY turn on “Active” (vs. passive) if you absolutely need to prevent execution prior to getting the disposition. (This is on a machine which you know to be infected.)



AMP4E Deployment Tips (Continued)

- Upgrade to latest version so the client will not require a reboot for future upgrades. There are lots of other bugfixes, too.
- When doing the Endpoint IoC scan, remember that it's very resource-intensive, and you should limit it only to the infections you think you might have, and only on machines you suspect are infected.
- When deploying to Windows servers, you **MUST** use the `/skipdfc 1` `/skiptetra 1` commands. This will avoid unexpected BSOD!

Integration with Cisco NGFW with Malware

Indications of Compromise (switch workflow)

Indications of Compromise Summary > **Indications of Compromise Details**

No Search Constraints ([Edit Search](#))

Jump to... ▼

☐	Category	Event Type
↓ ☐	Malware Download	Security Intelligence Event - DNS Malware
↓ ☐	Malware Detected	Threat Detected in File Transfer
↓ ☐	CnC Connected	Intrusion Event - malware-cnc
↓ ☐	Impact 2 Attack	Impact 2 Intrusion Event - attempted-admin
↓ ☐	CnC Connected	Security Intelligence Event - DNS CnC
↓ ☐	Exploit Kit	Intrusion Event - exploit-kit
↓ ☐	Impact 1 Attack	Impact 1 Intrusion Event - successful-user
↓ ☐	Impact 1 Attack	Impact 1 Intrusion Event - attempted-user
↓ ☐	Impact 2 Attack	Impact 2 Intrusion Event - web-application-attack
↓ ☐	Impact 2 Attack	Impact 2 Intrusion Event - attempted-user
↓ ☐	Impact 1 Attack	Impact 1 Intrusion Event - attempted-admin
↓ ☐	CnC Connected	Security Intelligence Event - CnC
↓ ☐	CnC Connected	Intrusion Event - malware-backdoor
↓ ☐	Malware Detected	Threat Detected by AMP for Endpoints - Not Executed

AMP Management

Dynamic Analysis Connections

[+ Add AMP Cloud Connection](#)

Cloud Name	Cisco AMP Solution Type	State	Actions
US Cloud (Global)	AMP for Endpoints and AMP for Networks	☒	

AMP4E detected threat reported in FMC
IoCs and can include OpenIoCs

Integration with Cisco NGFW with Malware

Containment

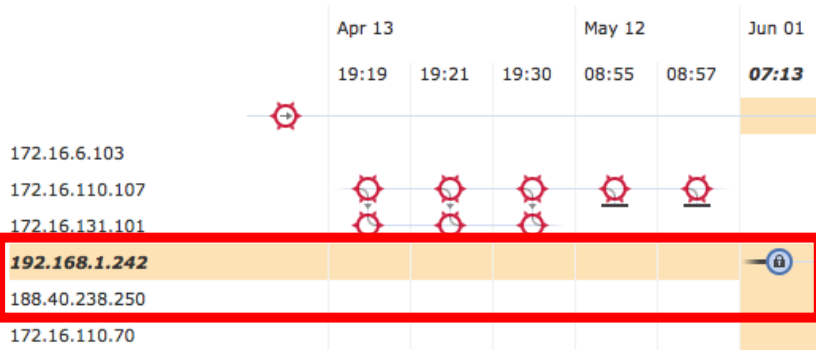
Eradication

Network File Trajectory for 275a021b...f651fd0f

File SHA256 275a021b...f651fd0f   
File Names [/eicar.com](#) , [/eicar/eicar.com](#) , [3328.tmp](#) , [4A9F.tmp](#) (+28 more)
File Size (KB) [0.0664](#)
File Type [TEXT UTF8](#)
File Category
Parent Applications [chrome.exe](#) , [firefox](#) , [firefox.exe](#)
Current Disposition  [Malware](#) 
Threat Score None
Detection Name [EICAR:EICAR_Test_file_not_a_virus-tpd](#)

First Seen 2015-10-15 17:34:01 on
Last Seen 2016-06-06 16:08:46 on
Event Count 76
Seen On 7 hosts
Seen On Breakdown 3 senders → 5 receivers (2 → 1 displayed)

Trajectory



Time 2016-06-01 07:13:36
Event Type File Quarantined
IP Address  [192.168.1.242](#)
Disposition  [Malware](#)
Action

Events  Transfer  Block  Create  Move  Execute  Scan  Retrospective  Quarantine
Dispositions  Unknown  Malware  Clean  Custom  Unavailable

Network Visibility Module (NVM) Details



NVM Configuration

- Module deployed via ASA from Group Policy

Optional Client Modules to Download:	☐ Inherit	nvm
Always-On VPN:	☒ Inherit	☐ AnyConnect DART
Client Profiles to Download:	☐ Inherit	☐ AnyConnect AMP Enabler
	☒ Add ☐ Delete	☒ AnyConnect Network Visibility
	Profile Name	☐ AnyConnect SBL
	nvm	☐ AnyConnect Posture
	vpn2	☐ AnyConnect Web Security
		☐ AnyConnect Network Access Manager
		☐ AnyConnect ISE Posture

NVM Configuration

- Module Deployed via ISE



Agent Resources From Local Disk > Agent Resources From Local Disk

Agent Resources From Local Disk

Category: Customer Created Packages

Type: AnyConnect Profile

* Name: NVM

Description: XML configuration file for Network Visibility Module

Browse... NVM_ServiceProfile.xml



AnyConnect Configuration > AnyConnect Configuration

* Select AnyConnect Package: AnyConnectDesktopOSX 4.2.96.0

* Configuration Name: AnyConnect ISE Posture and NVM

Description:

Description Value

* Compliance Module: AnyConnectComplianceModuleOSX 3.6.10255.2

AnyConnect Module Selection

ISE Posture ☒ Requires ISE Posture

VPN ☐

Web Security ☐

AMP Enabler ☐

Network Visibility ☒

ASA Posture ☐

Diagnostics and Reporting Tool ☐

Profile Selection

* ISE Posture: AnyConnect ISE Posture

VPN

Web Security

AMP Enabler

Network Visibility: NVM

Customer Feedback



mac_posture_nvm If Any and Mac OSX and Condition(s) then AnyConnect ISE Posture and NVM

NVM Configuration Template

Suppression and Throttling



Profile: ...ty\ciscolive\anyconnect 4.3 with ODNS\NVM_ServiceProfile.xml

Collector Configuration

IP Address/FQDN

Port

Aggregation Interval seconds

Throttle Rate Kbps

Note: Valid range: 12 - 2048. To disable: 0.

Collection Mode

Collection Criteria ☒ Broadcast packets ☒ Multicast packets

Data Collection Policy

Throttling so not to overwhelm VPN

All Networks
Off
Trusted Network Only
Untrusted Network Only
All Networks

Broadcast and Multicast Suppression

NVM Configuration Template

Flexible Data Collection Policy



Data Collection Policy

Name:

Network Type ☒ Vpn ☒ Trusted ☒ Untrusted

Type ☒ Include ☐ Exclude

Fields

- ☒ LoggedInUser
- ☒ ProcessName
- ☒ ProcessAccount
- ☒ ProcessHash
- ☒ ParentProcessName
- ☒ ParentProcessAccount

- ☒ ParentProcessHash
- ☒ DestinationHostname
- ☒ DNSSuffix
- ☒ L4ByteCountIn
- ☒ L4ByteCountOut
- ☒ VirtualStationName

- ☒ ModuleHashList
- ☒ InterfaceIndex
- ☒ InterfaceType
- ☒ InterfaceName

- ☒ OSName
- ☒ OSVersion
- ☒ SystemManufacturer
- ☒ SystemType
- ☒ OSEdition
- ☒ ModuleNameList





NVM Configuration Template

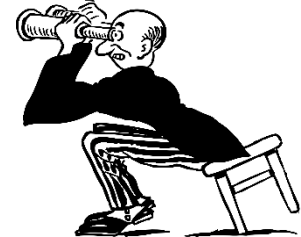
AnyConnect Profile Editor or ASDM

```
<?xml version="1.0" encoding="UTF-8"?>
<NVMProfile
  xsi:noNamespaceSchemaLocation="NVMProfile.xsd"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance">
  <CollectorConfiguration>
    <CollectorIP>fc.ciscolive.com</CollectorIP>
    <Port>2055</Port>
  </CollectorConfiguration>
    <AggInterval>5</AggInterval>
    <ThrottleRate>500</ThrottleRate>
    <CollectionMode>all</CollectionMode>
  <CollectionCriteria>
    <Broadcast>true</Broadcast>
    <Multicast>true</Multicast>
  </CollectionCriteria>
```

```
<DataCollectionPolicy>
  <Policy>
    <PolicyName>ALL_DataCollectionPolicy</PolicyName>
  >
    <NetworkType>VPN,Trusted,Untrusted</NetworkType>
  >
    <Type>include</Type>
    <Fields>12352,12353,12356,12357,12358,12333,12334,12335,1
    2336,12337,12338,12339,12340,12341,12342,12343,12344,123
    45,12346,12347,350,12351
  </Fields>
  </Policy>
</DataCollectionPolicy>
</NVMProfile>
```

Verify Application Versions Allowed

AnyConnect NVM with Stealthwatch



Outlook 2011 is allowed in my environment

```
MacOS$ shasum -a 256  
b041680eefdae88d9c4b78a6da81c134737574f  
270bcc3889b97f45344d66fa7 Microsoft  
Outlook
```

Run Flow Query on above hash

Run Flow Query on Application (Process Name) to see different versions (hashes)

Dec 15, 2015 8:13:44 AM	Dec 15, 2015 8:18:15 AM	4m 31s	Client	172.16.31.6	10.0.0.6	Microsoft Outlook	B041680EFDAAE88D9C4B78A6DA81C134737574F270BCC
Dec 14, 2015 4:32:03 PM	Dec 14, 2015 5:00:40 PM	28m 37s	Client	192.168.1.17	10.0.0.6	Microsoft Outlook	B041680EFDAAE88D9C4B78A6DA81C134737574F270BCC
Dec 15, 2015 10:28:52 AM	Dec 15, 2015 10:42:59 AM	14m 7s	Client	172.16.31.9	10.0.0.6	Microsoft Outlook	B041680EFDAAE88D9C4B78A6DA81C134737574F270BCC
Dec 15, 2015 7:55:14 AM	Dec 15, 2015 8:12:30 AM	17m 16s	Client	192.168.1.17	10.0.0.6	Microsoft Outlook	B041680EFDAAE88D9C4B78A6DA81C134737574F270BCC
Dec 15, 2015 10:28:51 AM	Dec 15, 2015 10:43:31 AM	14m 40s	Client	172.16.31.9	10.0.0.6	Microsoft Outlook	B041680EFDAAE88D9C4B78A6DA81C134737574F270BCC
Dec 15, 2015 8:13:41 AM	Dec 15, 2015 8:19:20 AM	5m 39s	Client	172.16.31.6	10.0.0.6	Microsoft Outlook	B041680EFDAAE88D9C4B78A6DA81C134737574F270BCC
Dec 14, 2015 4:41:40 PM	Dec 14, 2015 5:01:13 PM	19m 33s	Client	192.168.1.17	10.0.0.6	Microsoft Outlook	B041680EFDAAE88D9C4B78A6DA81C134737574F270BCC
Dec 15, 2015 10:45:43 AM	Dec 15, 2015 10:54:49 AM	9m 6s	Client	172.16.31.9	10.0.0.6	Microsoft Outlook	B041680EFDAAE88D9C4B78A6DA81C134737574F270BCC
Dec 15, 2015 10:45:43 AM	Dec 15, 2015 10:50:04 AM	4m 21s	Client	172.16.31.9	10.0.0.6	Microsoft Outlook	B041680EFDAAE88D9C4B78A6DA81C134737574F270BCC
Dec 14, 2015 4:53:34 PM	Dec 14, 2015 4:53:55 PM	21s	Client	172.16.31.3	10.0.0.6	Microsoft Outlook	B041680EFDAAE88D9C4B78A6DA81C134737574F270BCC

Network Visibility Module

Pros



- Application details – 100% accuracy verified against SHA256
- User Identity even from non-domain members
- Encryption Visibility without decryption

Cons



- Also needs other IPFix (netflow) devices with stealthwatch.
- Only visibility based on ingress/egress to client.



Complying with Corporate Policy

How do you Comply with Corporate Policy



Compliance software

- Windows Group Policy and SCCM (or 3rd party) for Windows
- JAMF/Casper e.g for MAC
- Enterprise Mobility Management – Cisco **Meraki**, MobileIron, Airwatch...etc

Integration with Policy

- ***Identity and Access Control***
- ***Remote Access VPN***

Compliance (Posture)

- Provides deep inspection in OS, File, Certificate, Registry, Anti-Virus, Anti-Spyware, Person Firewall, Ports open, Running processes...etc



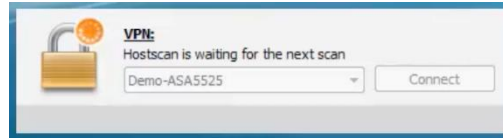
Anyconnect Apex license required!

Options

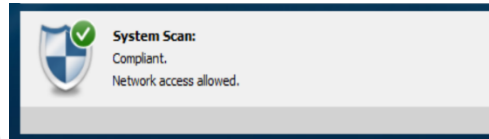
- Hostscan with



VPN connecting to an ASA Firewall



- ISE Posture with
Cisco live!



connecting to Wired, Wireless or VPN using

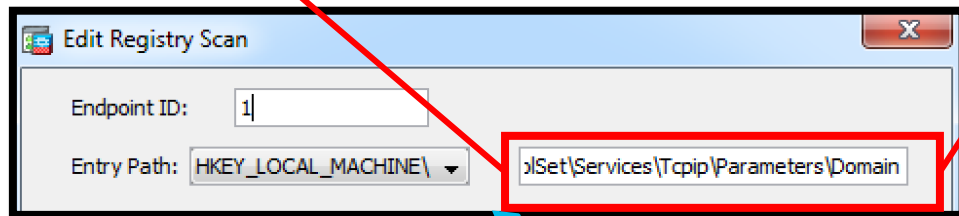




ASA Hostscan – Define Registry Scan

Machine Joined to Domain to ciscolive.demo

SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Domain



Defined attribute in ASDM under
Configuration > Remote Access
VPN > Secure Desktop Manager >
Host Scan



Dynamic
Access
Policy



ASA Hostscan – Dynamic Access Policy

Machine Joined to Domain to ciscolive.demo

Edit Dynamic Access Policy

Policy Name: Machine Joined to Domain

Description:

ACL Priority: 0

Selection Criteria

Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA at below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advance specify the logical expression text.

User has ALL of the following AAA Attributes values...

AAA Attribute	Operation/Value

Add Edit Delete

and the following endpoint attributes are satisfied.

Endpoint ID	Name/Operation/Value
registry.1	exists = true type = string value = ciscolive.demo

Edit Endpoint Attribute

Endpoint Attribute Type: Registry

☒ Exists ☐ Does not exist

Endpoint ID: 1

☒ Value: string = ciscolive.demo

☒ Caseless

OK Cancel Help



ISE Posture

Registry check for Machine joined to Domain

With ASA 9.2, inline Posture node is not required. Change of Authorisation is natively supported option

Registry Conditions List > **Domain_Check**

Registry Condition

* Name	Domain_Check		
Description	Check registry for Machine joined		
Registry Type	RegistryValue		
Registry Root Key	HKLM	* Sub Key	SYSTEM\CurrentControlSet\Service
* Value Name	Domain		
Value DataType	String		
Value Operator	does not equal		
Value Data	CISCOLIVE.DEMO		
* Operating System	Windows All		

Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements
	Policy_Check_For_Machine_Joined_to_Do main	If Any	and Windows All		then Joined_to_CiscoLive_D omain

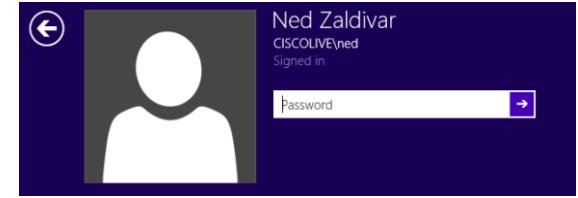
Endpoint Visibility	ASA Hostscan (Posture)	ISE Posture
Policy Framework	Dynamic Access Policy	ISE+VPN
Updates	Every 3 months	Dynamically
IP, Hostname, Mac address	Yes	Yes
Certificate Fields	Yes	Yes
BIOS Serial Number	Yes	Yes
Personal Firewall	Yes	Roadmap
File CRC32 Check	Yes	Yes
Disk Encryption	Roadmap	Yes
SHA256 File Check	Roadmap	Yes
USB Check	Roadmap	Yes*
Application	Roadmap	Yes, ISE 2.2
Stealth Agent	Roadmap	Yes
OS Support	Windows, Mac, Linux	Windows, Mac



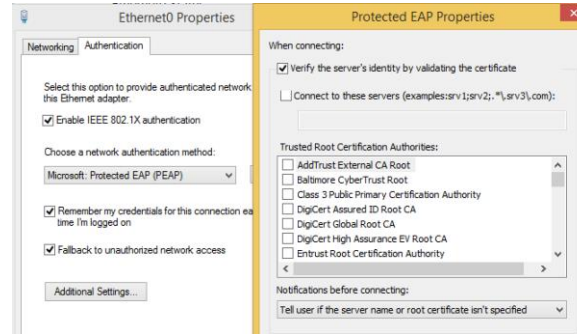
Connecting to Corporate Applications

Connecting to Corporate Applications

- Authenticated or Un-Authenticated Network Access



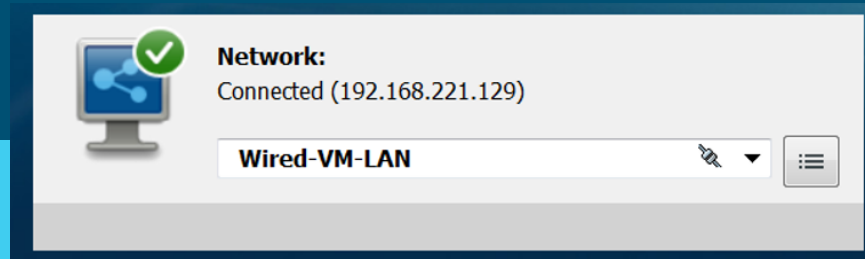
- Supplicant/Client programming



- Privacy of connection

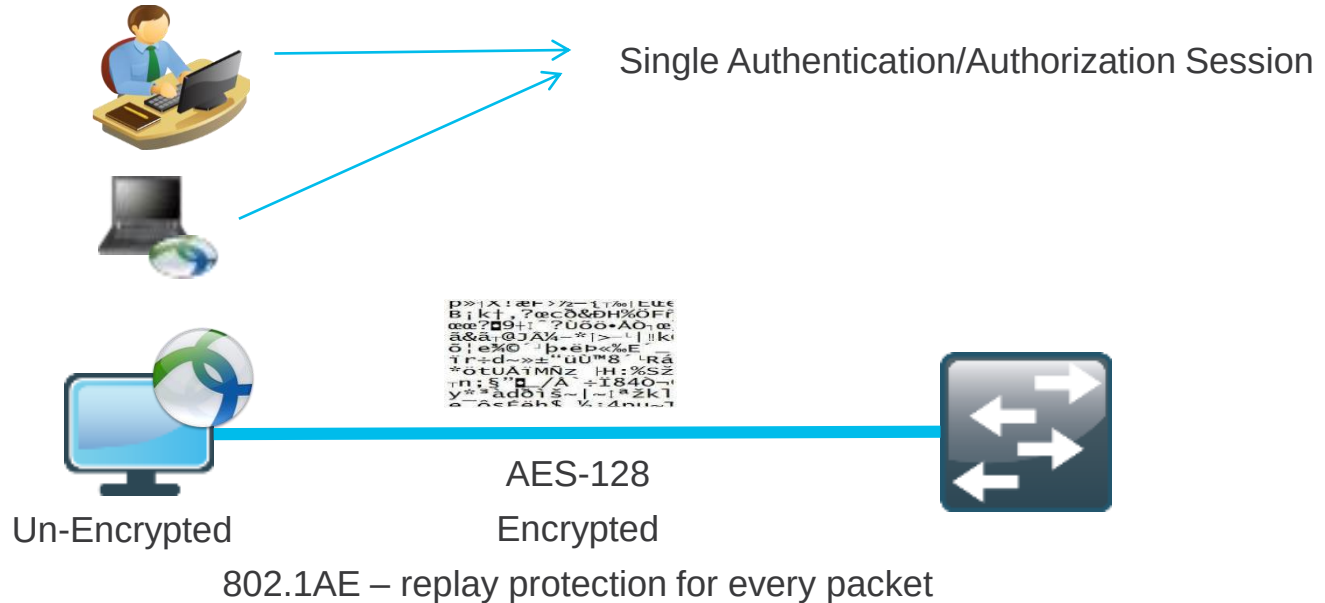


Network Access Manager



What is Network Access Manager (Windows Only)

- 802.1x Supplicant
- EAP-Chaining
- MacSEC



EAP-FAST (Flexible Authentication via Secure Tunnelling)

- Defined in RFC 4851 and was developed by Cisco Systems
 - Does not use certificates (anonymous PAC provisioning)
 - Mutual authentication provided by Protected Access Credential (PAC) file, usually provisioned dynamically
 - Anonymous versus Authenticated PAC Provisioning
 - Occurs in 3 Phases:
 - Phase 0: PAC Provisioning
 - Phase 1: Establishment of secure TLS tunnel using PAC
 - Phase 2: Inner authentication method for credential exchange
- Tunnel EAP(TEAP) in IETF draft, <https://tools.ietf.org/html/draft-ietf-emu-eap-tunnel-method-03>

EAP-Chaining – ISE Log Example

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	IP Address	Network Device	Authorization Profiles	Event	Auth Method	Authentication Protocol
2014-02-24 13:21:03.485	✓	 Win7 >> WIN7-VM			00:50:B6:0D:87:E5	Microsoft-Workstation	10.10.11.102	3560CG	Allow_All	Authentication succe...	dot1x	EAP-FAST (EAP-TLS)

Overview

Event	5200 Authentication succeeded
Username	Win7,WIN7-VM
Endpoint Id	00:50:B6:0D:87:E5
Endpoint Profile	Microsoft-Workstation
Authorization Profile	Allow_All
AccessSessionID	2/182636225/75;
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default

• User and Machine Tied together

• EAP-FAST Required



MacSec ISE Configuration Example

ISE Authorisation Result is MacSEC

☒ Employees if Employees then **MACSec Authz AND EMPLOYEES_SGT**

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template ☐

Track Movement ☐

Passive Identity Tracking ☐

Common Tasks

☒ MACSec Policy should-secure

ISE Authorization
Policy

~~must-not-secure~~
must-secure
should-secure

MacSec AnyConnect Configuration Example

The image shows the Cisco AnyConnect configuration window. The title bar says "Cisco AnyConnect". Below the title bar, it says "Enter information for the connection." The "Media:" section has two radio buttons: "Wi-Fi" and "Wired". The "Wired" button is selected and highlighted with a red box. Below "Media:", there is a checkbox for "Hidden Network". The "Descriptive Name:" field contains the text "MacSEC". The "SSID:" field is empty. The "Security:" dropdown menu is open, showing "802.1X (MACsec)" selected, which is also highlighted with a red box. Below the "Security:" dropdown, there is a section for "802.1X Configuration". It has two dropdown menus: the first is set to "password" and has a dropdown menu open showing "password", "certificate", and "token"; the second is set to "EAP-FAST". At the bottom, there is a text field for "Run this script on connection (optional):" and a button with three dots. At the very bottom are "OK" and "Cancel" buttons.

Wired Networks Only

Required Security

Any Authentication can be used

Network Access Manager:

Pros



- Full featured supplicant
- Privacy of traffic, but still able to inspect (macsec)
- Protects against spoofed user or corporate machine (eap-chaining)

Cons



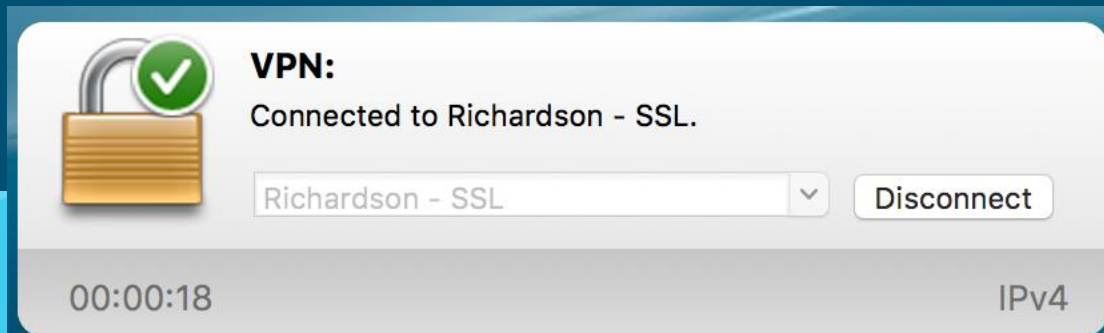
- Only available on Windows
- Requires coordination between Network, Security (switch, ISE) and Endpoint teams.



Cisco on Cisco Case Study

http://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/ISE_Cisco_on_Cisco_Trends_in_IT.html

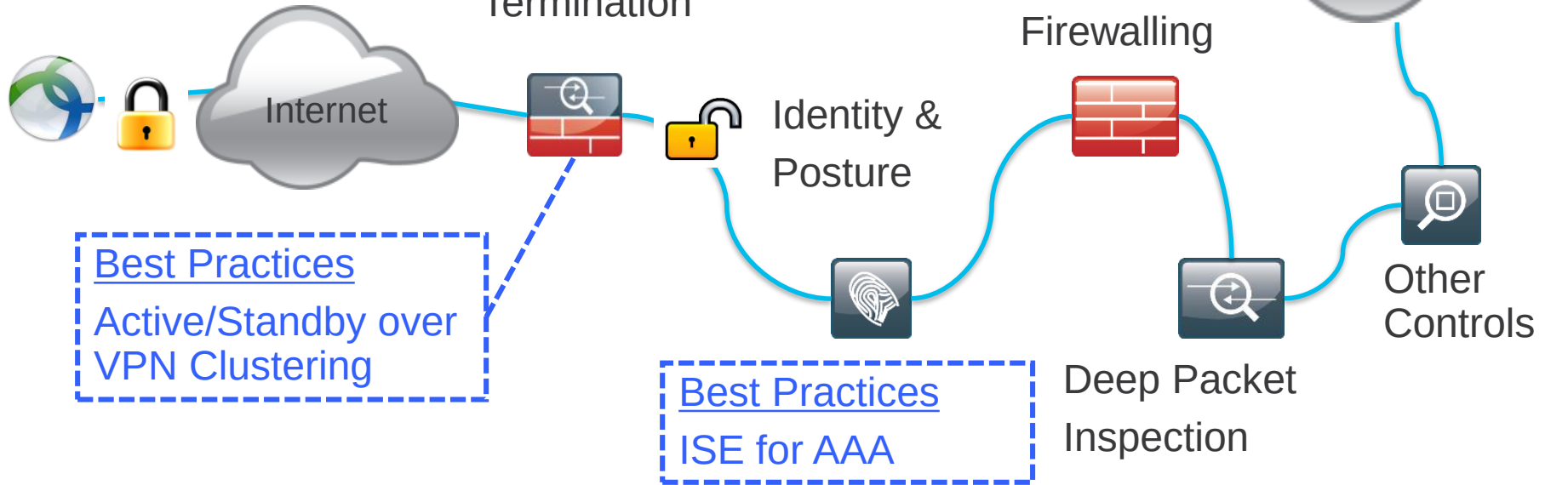
Remote Access VPN



Remote Access VPN

Allows for Centralised Security Controls

AnyConnect
VPN Tunnel



AnyConnect VPN Popular Features

- VPN Protocols– IPsec (IKEv2) and SSL (TLS 1.2)
- High Availability and Clustering - Optimal Gateway Selection, VPN Load balancing, A/S, Global Load Balancing

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	☒	☒	☒	☒

Configuration > Device Management > High Availability and Scalability > VPN Load Balancing

☒ Participate in Load Balancing Cluster

VPN Cluster Configuration

All servers in the cluster must get an identical cluster configuration.

Cluster IPv4 address: UDP port:

Cluster IPv6 address:

☐ Enable IPsec encryption

IPsec shared secret: Verify secret:

VPN Server Configuration

Public interface: Priority:

Private interface: NAT assigned IPv4 address:

NAT assigned IPv6 address:

As a VPN cluster master, this device can send a fully qualified domain name (FQDN) using reverse DNS lookup of a cluster device, instead of its outside IP address, when redirecting VPN client connections to that cluster device.

☒ Send FQDN to client instead of an IP address when redirecting

☒ Enable Optimal Gateway Selection ☒ User Controllable

Suspension Time Threshold (hours)

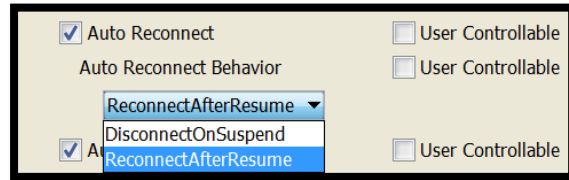
Performance Improvement Threshold (%)

OGS does not use simple
udp “ping” to RTT requests

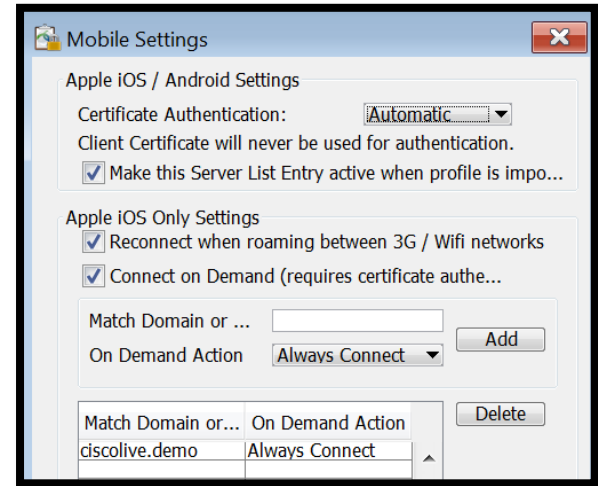
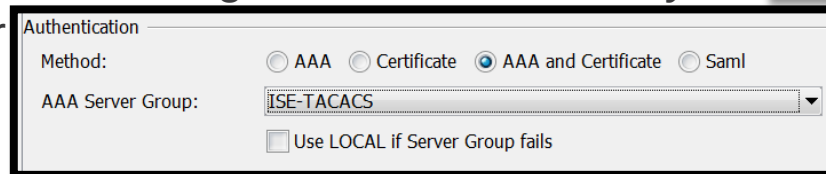
ASA cert with multiple SANS to prevent
untrusted popups!

AnyConnect VPN Popular Features

- Connect Options – Weblaunch, Full Client, Connect on Demand (Certificate only, DNS based, iOS only), Session Persistence/Pausing, PerApp VPN (Android and iOS), **Tunneled Default Gateway**



- Authentication – Username/Password (LDAP/AD, Radius), Certificates, Token, 2 Factor, Double Authentication
- Authorisation, Accounting – ACS or ISE or Any Radius Server



Recommended for Leveraging Centralised Controls

- ~~Manual requiring the enduser to manually connect to VPN.~~ 🤔
- Automatic using Always-On and Trusted Network Detection, requires little interaction. 😊



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile

☒ Automatic VPN Policy

Trusted Network Policy: Disconnect

Untrusted Network Policy: Connect

Trusted DNS Domains: *.ciscolive.demo

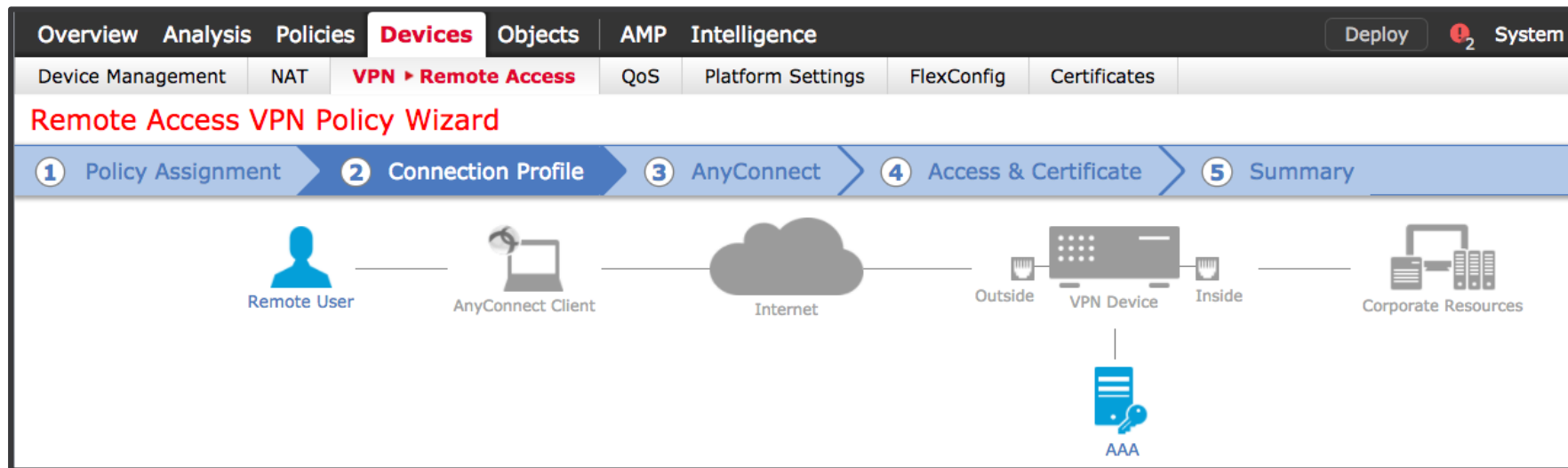
Trusted DNS Servers: 192.168.1.201, 192.168.1.202

Note: adding all DNS servers in use is recommended with Trusted Network Detection

Virtual Private Network (VPN)	
Statistics	Route Details
Firewall	Message History
▼ Control Frames	
Sent:	0
Received:	0
▼ Client Management	
Administrative Domain:	Undefined
Profile Name:	vpn2.xml
▼ Transport Information	
Protocol:	TLSv1.2
Cipher:	RSA_AES_128_SHA1
Compression:	None
Proxy Address:	No Proxy
▼ Feature Configuration	
FIPS Mode:	Disabled
Trusted Network Detection:	Enabled
Always On:	Disabled

Available on Cisco NGFW/Firepower Threat Defense

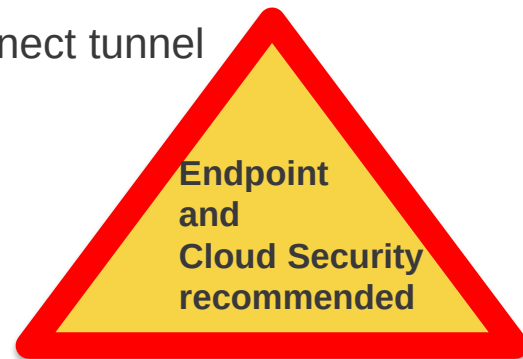
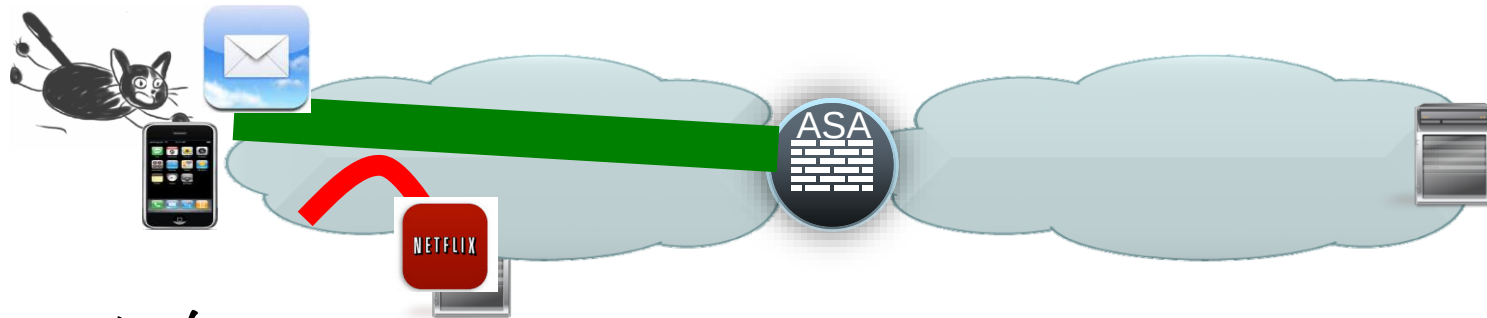
- First available on 6.2.1 for FPR 2100
- Available on all other Platforms with 6.2.2





Per App VPN

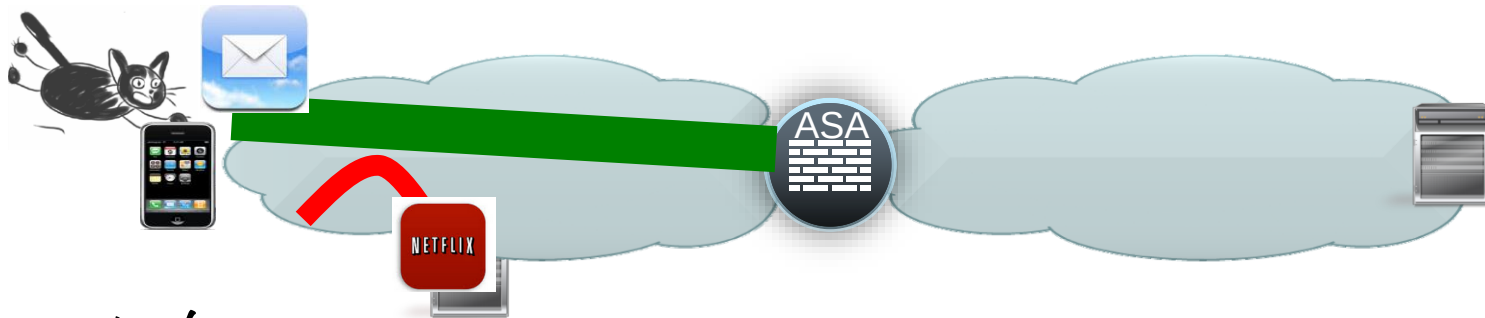
- Available for iOS 7.0+, Samsung Knox, Generic Android 5.0+
- Allows for tunneling specified subset of apps through one AnyConnect tunnel
 - save resources : don't Netflix over VPN tunnel
 - security: don't allow non enterprise apps on enterprise network
 - avoiding tunneling trusted cloud applications (to minimize latency)
- Configured via DAP
- Works with or without an Enterprise MDM





Dynamic Split Tunneling Exceptions

- AnyConnect 4.5 Windows and MAC
- Exclude specified DNS names from AnyConnect tunnel
 - save resources : don't Netflix over VPN tunnel
 - security: don't allow non enterprise apps on enterprise network
 - avoiding tunneling trusted cloud applications (to minimize latency)
- Configured via custom attributes



Remote Access with Centralised Controls:



Pros

- Least Expensive
- Leverages Expensive Tools at Central site



Cons

- Provides Limited visibility on Device
- Requires Full Tunnel for full Network Visibility
- Lack of flexibility
- Requires User to VPN, unless using TND/Always-On

Cisco on Cisco Case Study

<http://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/t-sec-05022016-transforming-the-enterprise-secure-mobility.html?cachemode=refresh>

Cloud Web Security

CWS - How does it Work?



80.254.145.118

Tower Selection



URL – www.yahoo.com

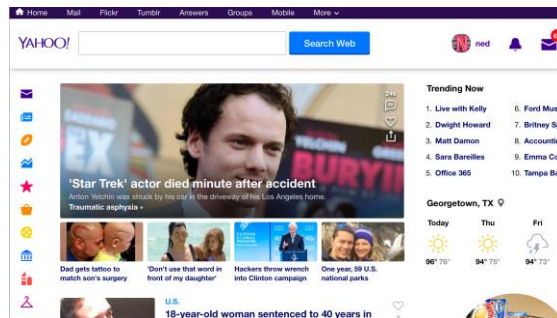
Web Filtering = Category = Search Engines and Portals

Web Reputation = Neutral, 60-70% block rates

Application Controls – Blocked download of Video

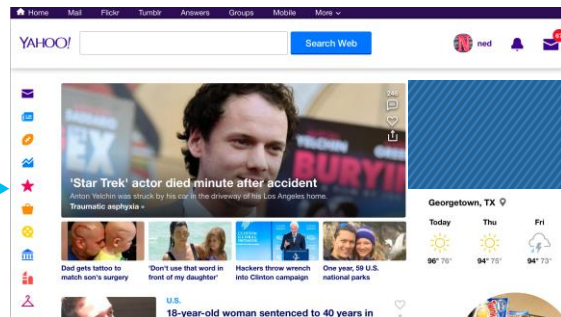
Anti-malware Scanning of File is downloaded = CLEAN

Outbreak Intelligence – bad content is blocked
but good content is still displayed



Select the activity for Vimeo to filter

- ☒ Download
- ☐ Post
- ☐ Upload



CWS - How does it Work? - Continued



Disposition = Unknown
File sent to Sandbox for
Dynamic Analysis

Cognitive Threat Analytics
(CTA) Confirmed your endpoint
is in a Campaign

Retrospective Alert -
w32.9ab7f9a2a7-100.sbx.vioc
Disposition = **Malware**

CONFIRMED **DETECTED**

10 #CMST04

100% confidence

7

AFFECTING

7 users , Windows

20+ users in 5+ companies

OCCURRENCE

32 days

May 15 - Jun 16

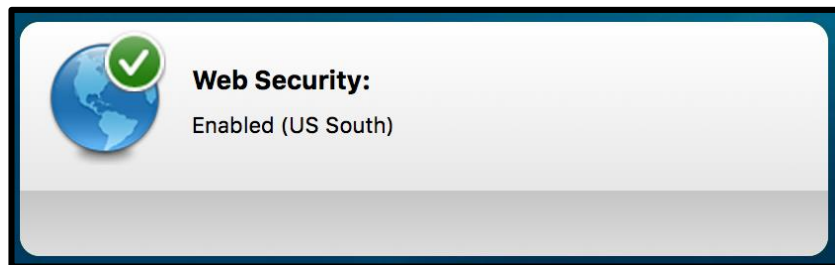
Add notes

Threat related to the Miuref and Boaxxe Trojan horse malware families. Threat is delivered via downloaders of the Zeus banking Trojan, exploit kits, and pay-per-install methods. Known for its information exfiltration capabilities, threat uploads data through HTTPS to external servers. Miuref can perform click-fraud by imitating the action of a user clicking on an advertisement. Click-jacking forces the user to websites that may potentially download additional malware such as Cryptolocker and banking Trojans. Perform a full scan of the infected device for the record and then reimage the device.

Threat Naming – AMP
www.talosintelligence.com/amp-naming/

What is AnyConnect Cloud Web Security (CWS)?

- Cloud Web Security is Proxy located in cloud for HTTP/HTTPS
- Cloud Managed, no on premise resources



- Provides Web Security while Mobile
- Supported on

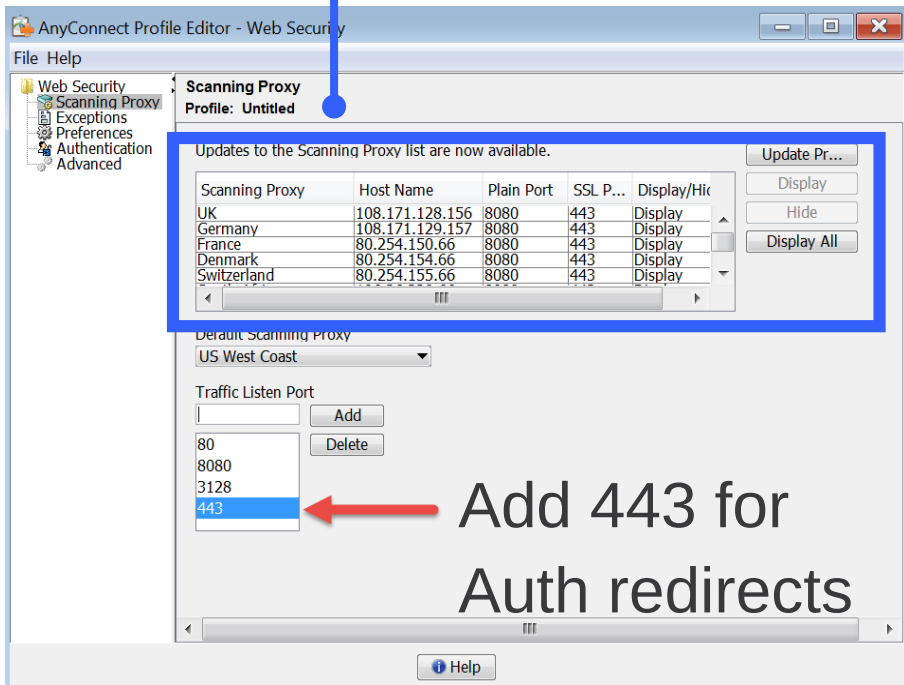


Cisco *live!*

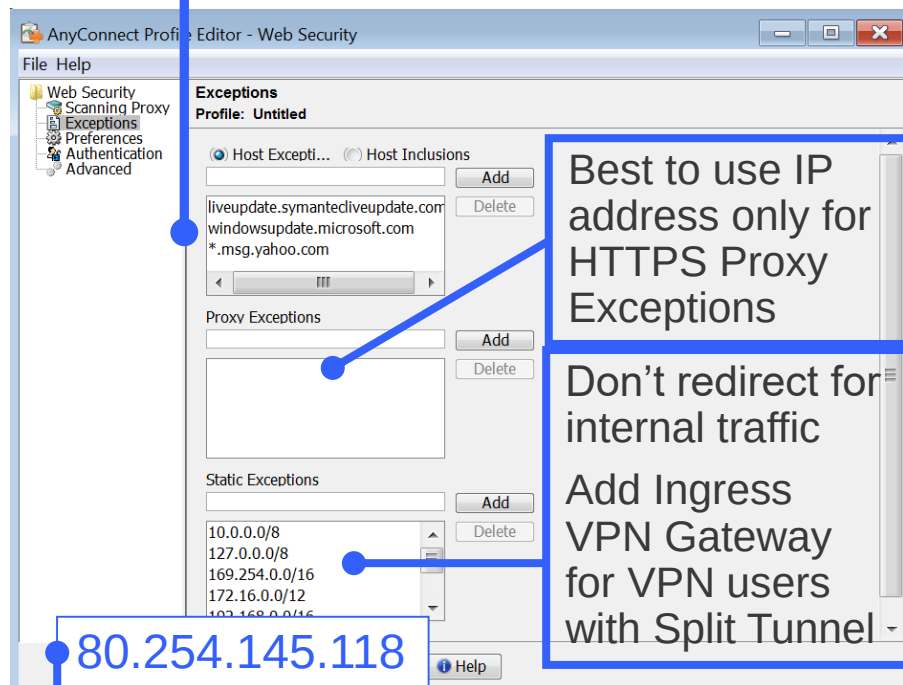


Deployment Configurations

Proxy Towers

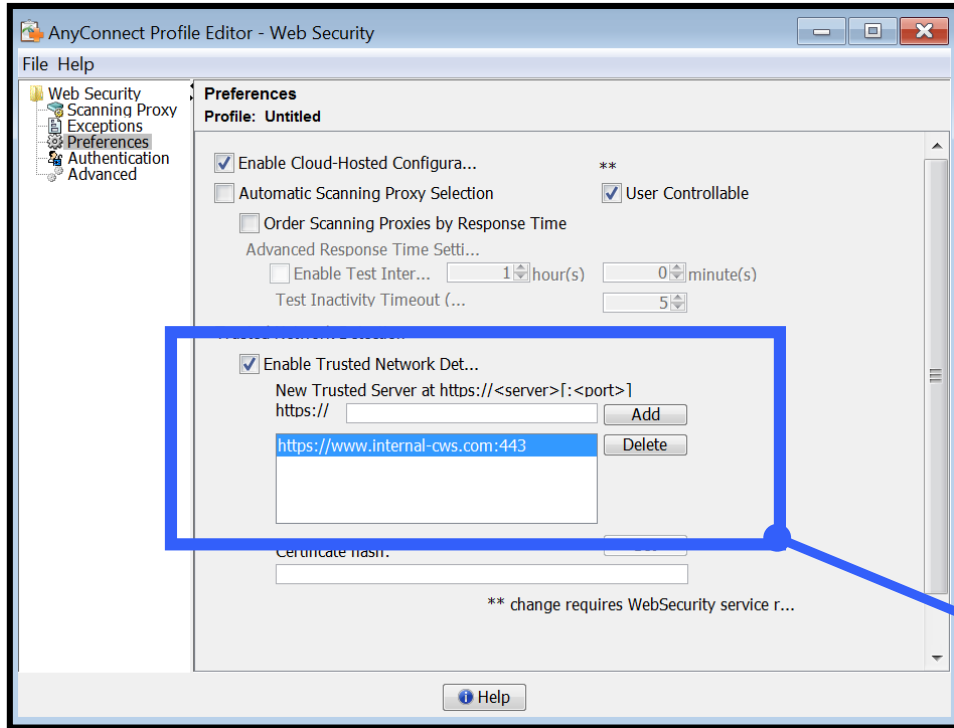


Exceptions

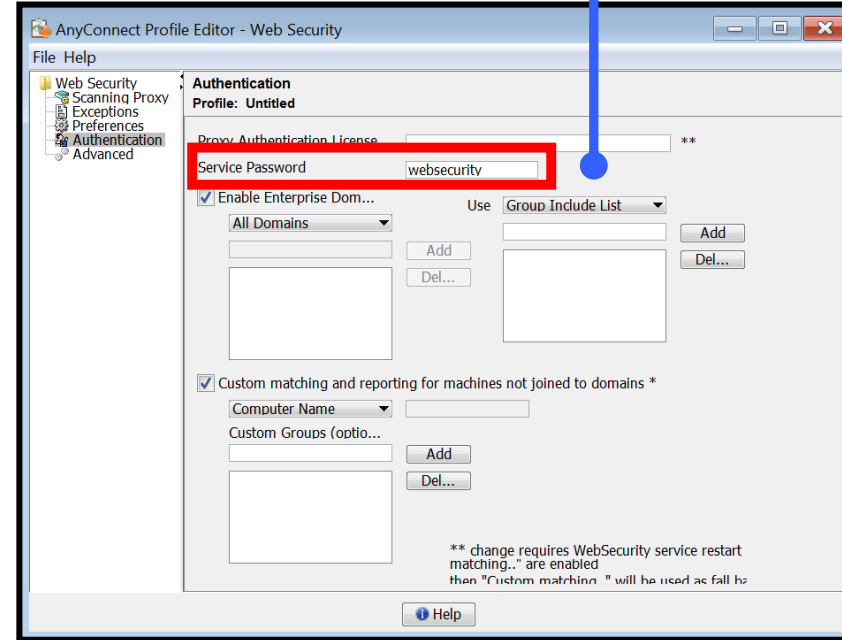


Auto Tower Check-In

Configuration Options



Prevent disabling CWS

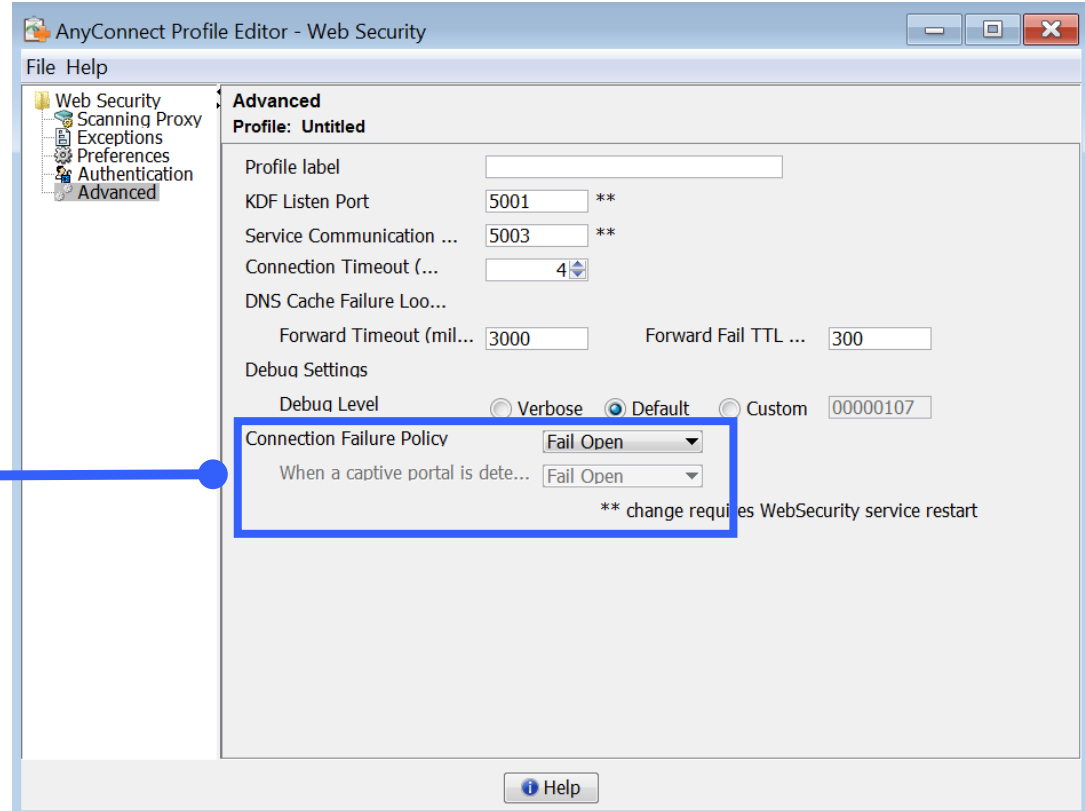


Disable CWS on corporate network!

Connection Failure Policy

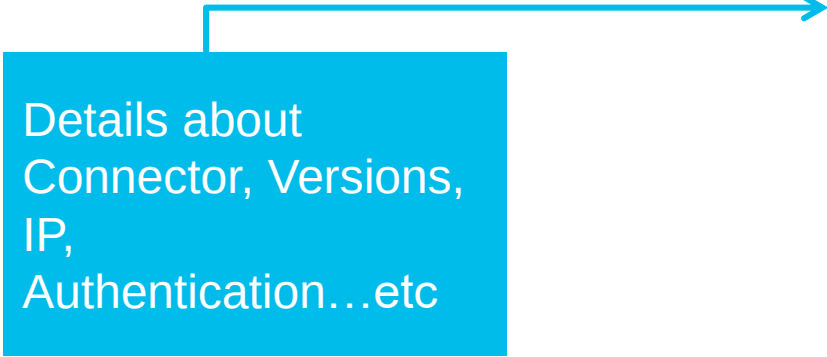
CWS failure?

Captive Portal at Hotel?



Am I Protected by CWS?

<http://whoami.scansafe.net>



Details about
Connector, Versions,
IP,
Authentication...etc

- authUserName: 192.168.1.19
- authenticated: true
- companyName: Internal_Development_Alpha
- connectorGuid:
440167D3B138F3AABDDA986A4E33C2A4
- connectorVersion: AP_AC4.3.01034
- countryCode: US
- externalIp: 76.30.241.47
- groupNames: alpha
- internalIp: 192.168.1.19
- logicalTowerNumber: 10330
- staticGroupNames: alpha
- userName: 192.168.1.19

CWS Management – <https://scancenter.scansafe.com>

Detection/Protection and Reporting



Select All Select None Add Filter

- ▶ Rule Action is equal to block
- ▶ SHA256 Source contains response

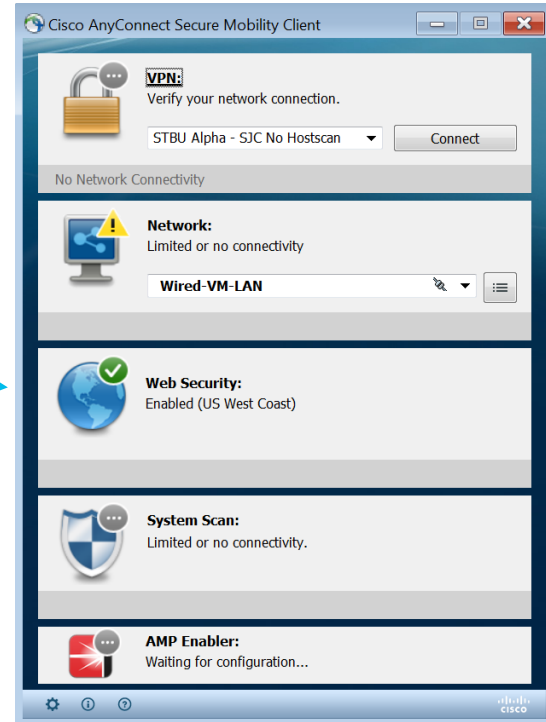
Malware has been detected and blocked inline

Timestamp	Path	AMP Threat Name	User	Internal IP	Rule Action
05-07-2016 11:16:52	/b/setup_3017e.exe	w32.b59a25ed27-100.sbx.vioc	winnt://demodata\marketing_user0	10.7.1.200	block
05-07-2016 09:07:14	/pgm/cafconsetup.exe	w32.adwaregen.18no.1201	winnt://demodata\marketing_user0	10.7.1.200	block
05-07-2016 08:09:31	/upgrade/2 0 18/pureleadssetup-2.0.18.exe	injector:autoit-tpd	winnt://demodata\finance_user1	10.7.1.101	block

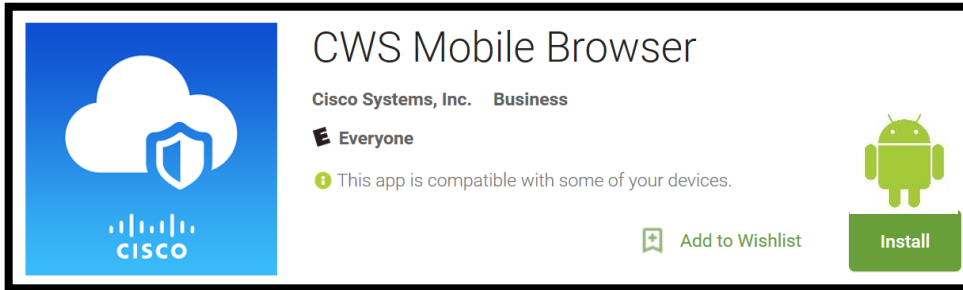
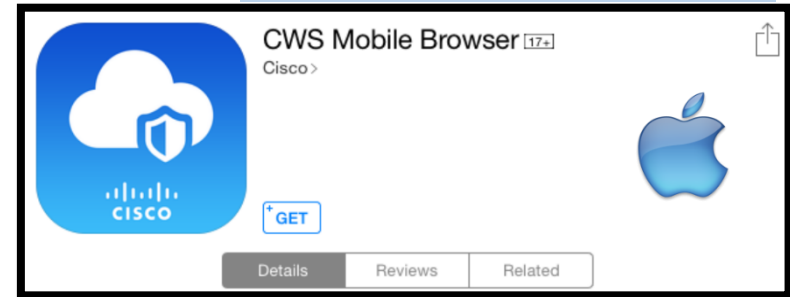
AMP Threat Name	Bandwidth (Bytes)	Browse Time (Min)	Bytes Received	Bytes Sent	Hits
Totals for AMP Threat Name	1,159,491,920	650	1,159,491,920	0	2,698
w32.0291725ebc-100.sbx.vioc	196,657,776	94	196,657,776	0	658
injector:autoit-tpd	557,297,664	93	557,297,664	0	651
w32.generickd:malwaregen.19dv.1201	114,933,760	92	114,933,760	0	460
w32.98b4ddd57a-100.sbx.tg	103,763,968	47	103,763,968	0	329
w32.33d12a79c8-99.sbx.vioc	98,918,400	46	98,918,400	0	322
w32.adwaregen.18no.1201	87,920,352	138	87,920,352	0	138
w32.auto.8bc6cb.mash.sr.sbx.vioc	0	47	0	0	47
w32.c618d8a14b-100.sbx.vioc	0	47	0	0	47
w32.b59a25ed27-100.sbx.vioc	0	46	0	0	46

CWS Deployment Options

- Windows and MacOSX
- Via Anyconnect 3.x/4.x



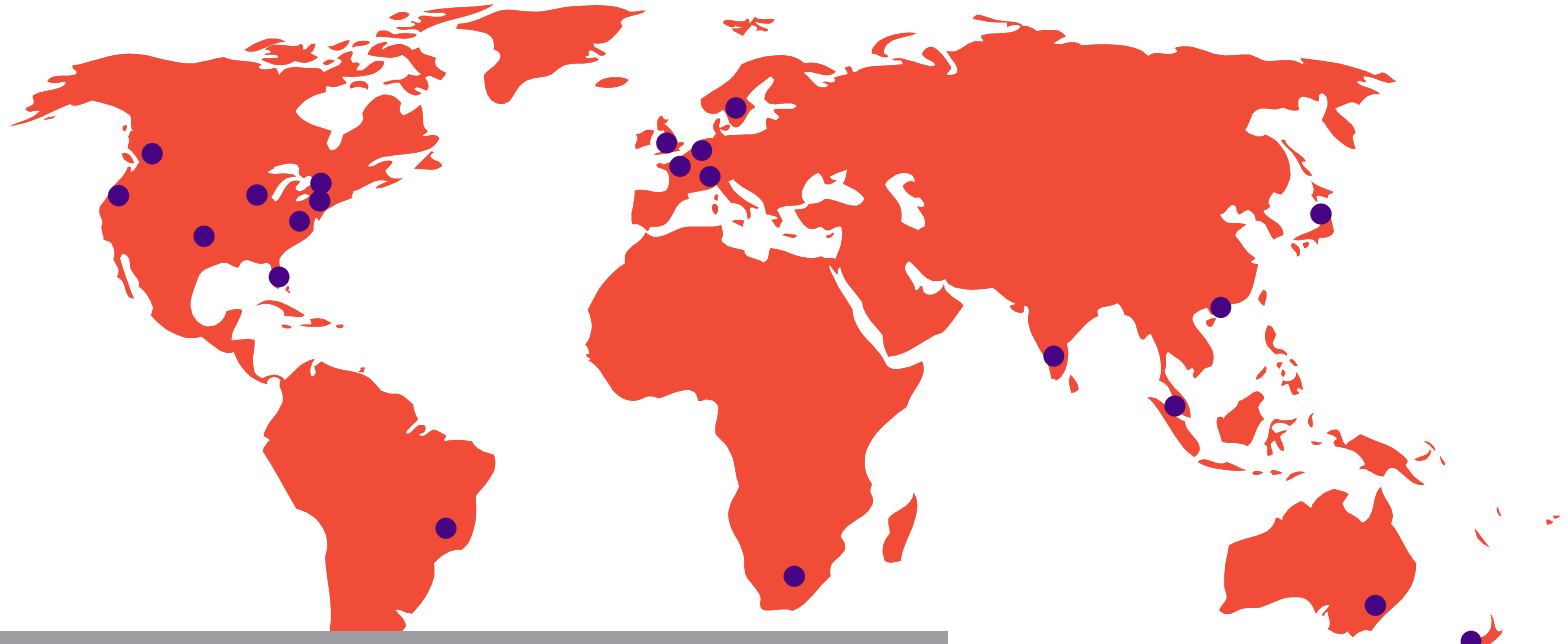
- CWS for Mobile (App Store or GooglePlay)



Cisco *live!*

Global Data Centre Footprint for CWS

<http://servicestatus.sco.cisco.com/status>



Current Data Centres

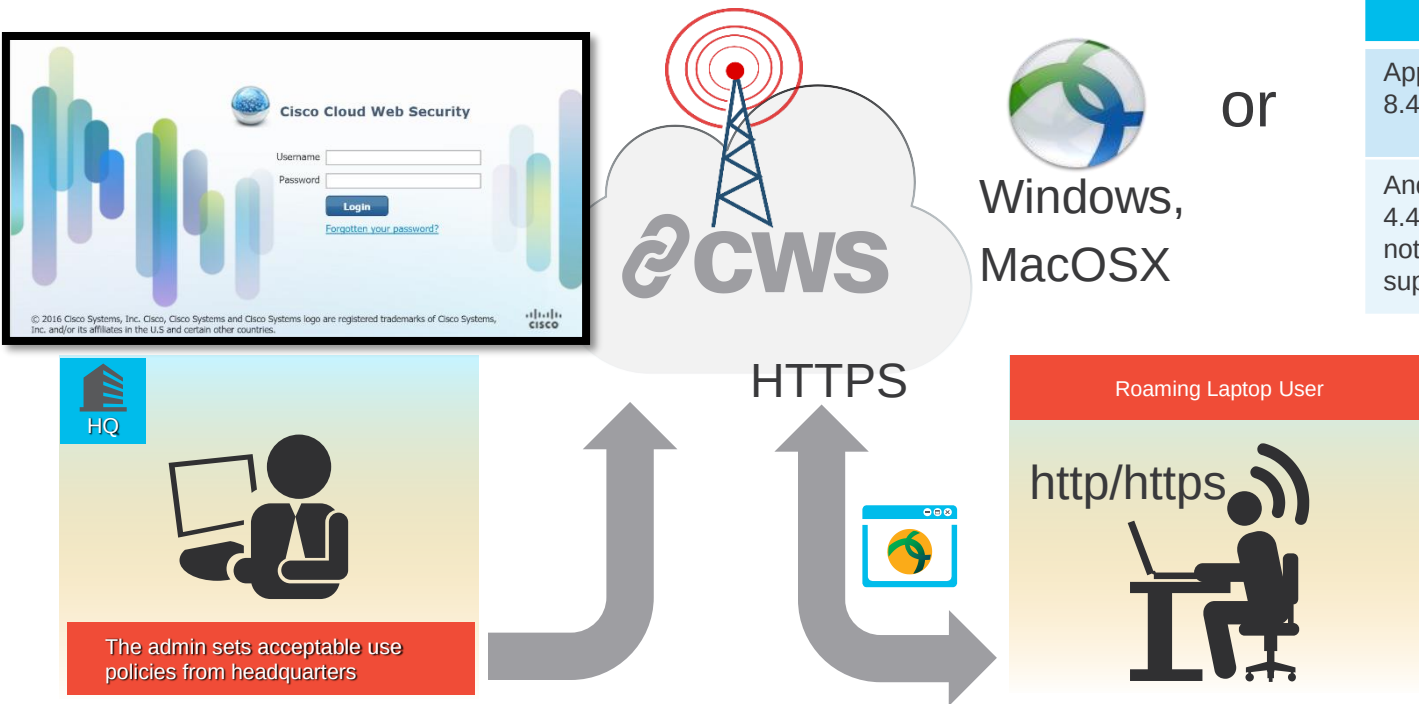
Auckland	Hong Kong	San Jose	Secaucus
Bangalore	Johannesburg	Sao Paulo	Toronto
Chicago	London (x2)	Singapore	Vancouver
Copenhagen	Miami	Sydney	Washington DC
Dallas	New Jersey (x2)	Tokyo	Christchurch
Frankfurt	Paris	Chennai	Zurich

CWS logs also available via S3 compatible API (w3c text format, 15 mins delay)

Extend CWS to Roaming Devices

CWS browser

OS	Mobile Devices
Apple iOS 8.4 +	iPad Mini, 3, 4, Air/2 (Pro not supported)
Android 4.4+ (6.0 not supported)	All mobile smartphone/tablets should be supported (except variants such as Kindle)



Cisco AnyConnect®:

- Enforces policies for all users, including those on roaming laptops
- Delivers the same CWS malware protection to roaming users as those at the branch office or main campus

Cloud Web Security:



Pros

- Protection from Web Threats (CWS)
- Deep controls including AVC
- CTA able to examine threats that need more data to pickup.
- AMP able to prevent and track bad files.
- Visibility/Control for Web – HTTPS/HTTP
- No need to upgrade, managed by Cisco.



Cons

- Only for HTTP/HTTPS



Cisco Security Connector Intro

Cisco Security Connector

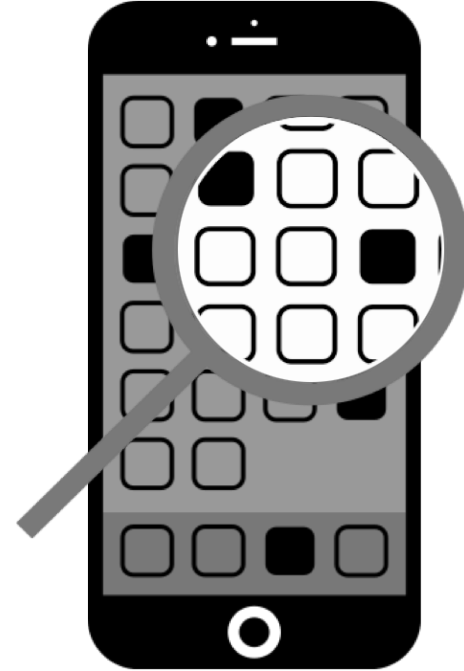
Security Extension to Apple/Cisco Partnership

- Extend **visibility**, **control**, and **privacy** for iOS
- Single app to enable additional security features
- Deploy to supervised devices through MDM solutions



Visibility – AMP4E like Functionality

- Gain insight into activity on iOS devices during incident investigations
- Build audit reports of user, device, and app traffic
- Quickly identify the impact and degree of risk exposure



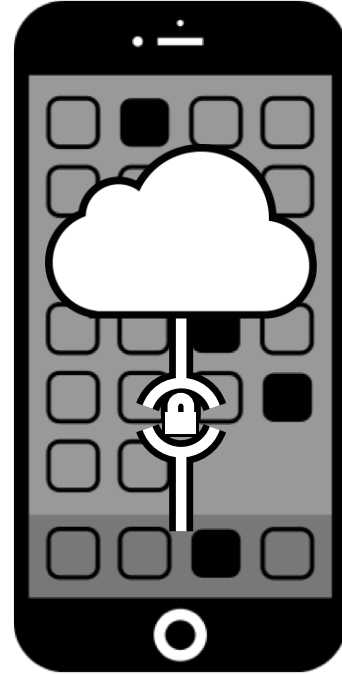
Control - Umbrella

- Protect users from connecting to malicious destinations
- Defend against phishing attacks and accidental browsing of bad sites
- Coverage on corporate networks, public Wi-Fi, and cellular networks



Privacy - Umbrella

- Ensure internet requests are encrypted on public Wi-Fi networks
- Protect requests from being intercepted and scanned
- Prevent communications from being intercepted and redirected



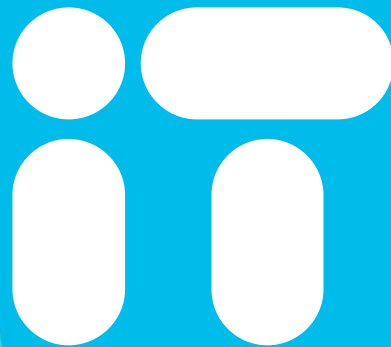


Cisco Security Connector Requirements

- ✓ Enterprise-owned iOS devices run in supervised mode (must belong to Apple's Volume Purchase Program (VPP))
- ✓ Cisco Meraki Systems Manager using the MDM system
 - ✓ Enable Clarity and Umbrella on iOS devices
 - ✓ Ensure devices are under management and actively share device information with Clarity and Umbrella
 - ✓ Licensed by number of devices
- ✓ Subscription to Cisco Umbrella (licensed per number of internet-connected users)
- ✓ Subscription to Cisco Clarity (AMP for Endpoints – licensed per device)



You're



Cisco *live!*