Cisco Umbrella

Design Guide

June, 2021
Overview

Security is shifting and converging in the cloud. You may hear different names for this trend such as secure internet gateway (SIG), edge security, Secure Access Service Edge (SASE), and more. It can get confusing.

Regardless of what you call it, it denotes: multiple security functions integrated in one cloud service; flexibility to deploy security services how and where you choose; ability to secure direct-to-internet access, cloud app usage and roaming users; plus, no appliances to deploy.

Cisco Umbrella is a cloud-delivered security service that brings together essential functions that you can adopt incrementally, at your pace. Umbrella unifies secure web gateway, DNS security, cloud-delivered firewall, cloud access security broker functionality, and threat intelligence. Deep inspection and control ensures compliance with acceptable-use web policies and protects against internet threats. Accelerated threat detection/response and centralized management makes it ideal for decentralized networks.

Figure 1. Cisco Umbrella SIG Overview
Solution Overview

Umbrella offers a broad set of security functions that until now required separate firewall, web gateway, threat intelligence, and cloud access security broker (CASB) solutions. By enabling all of this from a single, cloud-delivered service and dashboard, Umbrella significantly reduces the time, money, and resources previously required for deployment, configuration, and integration tasks. It can be integrated with your SD-WAN implementation to provide a unique combination of performance, security, and flexibility that delights both your end users and security team.

Packet flow through Umbrella SIG

The following components are integrated seamlessly in a single, cloud-delivered service:

- Umbrella DNS is resolved first. It is the first check for malicious or unwanted domains and is based on the defined DNS policies. This reduces the quantity of traffic that is sent to the CDFW and SWG, improving responsiveness and performance.
- All traffic that has made it through DNS checks will be inspected by the CDFW. The firewall provides visibility and control for outbound internet traffic across all ports and protocols (L3/L4) as well as L7.
- The SWG will inspect any traffic that is destined for 80/443 after it has been permitted by the CDFW to provide a deeper security inspection. It will also apply application, visibility and control policies.
DNS-Layer Security

This is the first line of defense against threats because DNS resolution is the first step in internet access. Enforcing security at the DNS and IP layers, Umbrella blocks requests to malicious and unwanted destinations before a connection is even established—stopping threats over any port or protocol before they reach your network or endpoints. As a cloud-delivered service, it:

- Provides the visibility needed to protect internet access across all network devices, office locations, and roaming users
- Logs and categorizes DNS activity by type of security threat or web content and the action taken—whether it was blocked or allowed
- Retains logs of all activity for 30 days (export for longer retention), ready to recall for deeper investigation
- Can be implemented quickly to cover thousands of locations and users in minutes, to provide immediate return on investment

This level of protection is enough for some locations and users, yet others need additional visibility and control to meet compliance regulations and further reduce risk.
Secure Web Gateway (SWG)

Umbrella includes a full cloud-based secure web gateway (proxy) that can log and inspect all of your web traffic for greater transparency, control, and protection. The SWG functionality includes:

- The ability to efficiently scan all downloaded files for malware and other threats using the Cisco Advanced Malware Protection (AMP) SHA hash lookups and additional anti-virus engines
- Full or selective SSL decryption to further protect your organization from hidden attacks and time-consuming infections
- Granular app controls to block specific user activities in select apps (e.g., file uploads to Dropbox, attachments to GMail, post/shares on Facebook)
- File type blocking (e.g., block download of .exe files)
- Detailed reporting with full URL addresses, network identity, allow or block actions, plus the external IP address
- Content filtering by category or specific URLs to block destinations that violate policies or compliance regulations
- Sandboxing of files using an integrated cloud delivered Threat Grid. When a file disposition is unknown by AV or AMP lookup the file is sent to the sandbox for deeper inspection

Connectivity using IPSec tunnels, PAC files, AnyConnect or proxy chaining can be used to forward traffic to Umbrella for full visibility, URL and application level controls, and advanced threat protection.
Cloud-Delivered Firewall (CDFW)

Figure 5. Umbrella CDFW capabilities
With Umbrella’s firewall, all activity is logged and unwanted traffic is blocked using IP, port, and protocol rules. To forward traffic, you simply configure an IPsec tunnel from any network device. Management is handled through the Umbrella dashboard, and as new tunnels are created, security policies can automatically be applied for easy setup and consistent enforcement throughout your environment. Umbrella’s cloud-delivered firewall provides:

- Visibility and control for internet traffic across all ports and protocols
- Scheduled policy rules
- Customizable IP, port, and protocol policies in the Umbrella dashboard
- Layer 7 (application layer) inspection and filtering, using the NBAR2 engine
- Automated reporting logs, including policy hit count
Cloud access security broker (CASB)

Out of band/API
- Cloudlock UEBA
- Cloudlock DLP
- Cloudlock Apps Firewall – OAuth-connected apps

Inline/Proxy
- Umbrella App Discovery & blocking
- Umbrella Advanced App Control
  - Block uploads Dropbox/Box
  - Block attachments Webmail

Figure 6. CASB types and capabilities
Umbrella Cloud Access Security Capabilities include the App Discovery report which helps expose shadow IT by detecting and reporting on the cloud applications in use across your environment. It automatically generates reports on the vendor, category, application name, and volume of activity for each discovered app. The detailed reports include risk information such as web reputation score, financial viability, and relevant compliance certifications. App Discovery provides:

- Extended visibility into cloud apps in use
- App details and risk information
- Ability to block/allow specific apps

Tenant Controls enable you to restrict the instance(s) of Software as a Service (SaaS) applications that all users or specific groups/individuals can access. For example, you are able to block access to all non-corporate instances of Microsoft Office O365, preventing users from re-sharing corporate data to their personal SaaS instances.

Threat Intelligence

Data
- Umbrella DNS data – 200B requests per day
- Cisco Talos feed of malicious domains, IPs, and URLs

Models
- Dozens of models continuously analyze millions of live events per second
- Automatically uncover malware, ransomware, and other threats

Security researchers
- Industry renown researchers
- Build models that can automatically classify and score domains and IPs

Figure 7. Investigate Threat Intelligence Triage
Umbrella analyzes over 200 billion DNS requests daily. We ingest this massive amount of internet activity data from our global network and continuously run statistical and machine learning models against it. Our unique view of the internet enables us to uncover malicious domains, IPs, and URLs before they’re used in attacks. Umbrella security researchers constantly analyze this information, and supplement it with intelligence from
Cisco Talos to discover and block an extensive range of threats. This threat intelligence powers not only Cisco Umbrella, but also your ability to respond to incidents. Your analysts can leverage Umbrella Investigate for rich intelligence about domains, IPs, and malware across the internet, enabling them to:

- Gain deeper visibility into threats with the most complete view of the internet
- Better prioritize incident investigations
- Speed incident investigations and response
- Predict future attack origins by pinpointing and mapping out attackers’ infrastructures
- Easily integrate Investigate data other security orchestration tools

Architecture Overview

Figure 8. Cisco Umbrella architecture

Umbrella is in alignment with the SAFE model that includes the domains for Management, Visibility, Segmentation, Secure Services, Threat Defense, and Compliance. Internet edge is an essential segment in the enterprise network, where the corporate network meets the public Internet. The SAFE Model identifies the Internet edge as one of the Places in the Network (PIN). SAFE simplifies 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 domain against those threats. Cisco has deployed, tested, and validated designs. These solutions provide guidance and best practices that ensure effective, secure remote access to resources.
The key to SAFE organizes the complexity of holistic security into PINs and Security Domains. The Internet edge is the highest-risk PIN because it is the primary ingress for public traffic and the primary egress point to the Internet. Simultaneously, it is a critical resource that businesses need in today’s Internet-based economy. SAFE matches up defensive capabilities against the categories of threats today. SAFE simplifies security by starting with business flows, then addressing their respective threats with corresponding security capabilities, architectures, and designs. SAFE provides guidance that is holistic and understandable.
Figure 10. Umbrella Design Guide location
More information about how Cisco SAFE simplifies security, along with this and other Cisco Validated Designs (CVD), can be found here: [www.cisco.com/go/safe](http://www.cisco.com/go/safe).
Umbrella Business Flows

SAFE uses the concept of business flows to simplify the identification of threats. This enables the selection of capabilities necessary to protect them. Traditionally, organisations routed internet traffic from branch offices back to a central location to apply security. Yet in today’s branch offices with high cloud application use, this centralized security approach has become impractical due to the high cost and performance issues of backhauling traffic. Many remote offices find ways to go direct to the internet for convenience and performance benefits.

Figure 11, SIG Business flows

Attack Surfaces

Umbrella provides security capabilities for the attack surfaces associated with the Internet PIN. For more details on SAFE capabilities, see the SAFE Overview Guide.
Figure 12. SIG Attack surfaces

Figure 13. Required security capabilities for SIG Business Flows

Umbrella Integrations

Figure 14. Umbrella Integrations

Umbrella, while providing multiple levels of defense against Internet-based threats, is the center piece of a larger architecture for Internet security. This section will explore the integrations that occur with other products in the Cisco portfolio and the role each plays in securing the business flows.
Cisco SD-WAN integration

Backhauling Internet bound traffic from remote sites is expensive and adds latency. Many organizations are upgrading their network infrastructure by adopting SD-WAN and enabling Direct Internet Access (DIA).

With the Umbrella and Cisco SD-WAN integration, you can simply and rapidly deploy Umbrella IPSec tunnels across your network and gain powerful cloud-delivered security to protect against threats on the Internet and secure cloud access. This market-leading automation makes it easy to deploy and manage the security environment over tens, hundreds or even thousands or remote sites. Umbrella’s DNS security also can be deployed with a single configuration in the Cisco SD-WAN vManage dashboard. When you need additional security and more granular controls, our integrated approach can efficiently protect your branch users, connected devices, and application usage at all DIA breakouts. Umbrella offers flexibility to create security policies based on the level of protection and visibility you need – all in the Umbrella dashboard.

Figure 15. Cisco SD-WAN with Umbrella SIG
Cisco SecureX Integration

Figure 16. Cisco SecureX

The Cisco SecureX platform connects the breadth of Cisco’s integrated security portfolio and additional third-party tools for a consistent, simplified experience to unify visibility, enable automation, and strengthen your security. It aggregates data from a multitude of Cisco and partner products for improved intelligence and faster response time. You can immediately visualize the threat and its organizational impact and get an at-a-glance verdict for the observables you are investigating through a visually intuitive relations graph. It enables you to triage, prioritize, track, and respond to high fidelity alerts through the built-in Incident Manager. Then you can take rapid response actions across multipletscurity products: isolate hosts, block files and domains, and block IPs – all from one convenient interface. SecureX empowers your security operations center (SOC) teams with a single console for direct remediation, access to threat intelligence, and tools like casebook and incident manager. It overcomes many challenges by making threat investigations faster, simpler, and more effective.

Cisco Advanced Malware Protection (AMP) and Threat Grid
Umbrella’s **File Analysis** features File Inspection and Threat Grid Malware Analysis – enabled through the DNS and Web policy wizards – inspect files for malicious content. To Umbrella, a risky domain is one that might potentially pose a threat because little or no information is known about it. It is a domain that is neither trusted or known to be malicious. Files can be encountered by Umbrella through an explicit download, such as when a user clicks a link in an email, or through a behind-the-scenes ‘drive-by’ download scenario. Once inspected, Umbrella allows "good" files through and blocks the downloading of malicious files. When a malicious file is detected, Umbrella’s block page is returned.

At any time you can review Umbrella’s inspection activities through the **Security Activity** and **Activity Search** reports.

Umbrella uses an AMP SHA hash lookup to scan for malicious files. AMP is built on an extensive collection of real-time threat intelligence and dynamic malware analytics supplied by the Talos Security Intelligence and Research Group, and Threat Grid intelligence feeds. The Cisco AMP engine does not do real-time sandboxing, instead, the Cisco AMP integration blocks files with a known bad reputation based on the checksum or hash of the file. The AMP checksum database is comprised of lookup and data from all AMP customers and is a dynamic global community resource shared between customers utilizing the technology. For more information about AMP, see [Advanced Malware Protection (AMP)](https://www.cisco.com/c/en/us/solutions/Security/AMP.html).
Cisco DUO Integration

**Figure 18. Cisco DUO Integration**
Umbrella is not an open proxy, and therefore must trust the source forwarding web traffic to it. This can be accomplished by assigning either a network or tunnel identity to a web policy. Policies created in this fashion apply broadly to any web traffic originating from the network or tunnel. However, to create more granular policies for users or groups, Security Assertion Markup Language (SAML) should be implemented or AnyConnect installed on the devices.

Identities obtained from SAML can be matched to users and groups which have been provisioned by manually importing a CSV file from Active Directory, or automatically by using Active Directory-based provisioning with the Umbrella AD Connector.

Duo Access Gateway acts as an IdP, authenticating your users using existing on-premises or cloud-based directory credentials and prompting for two-factor authentication before permitting access to your service provider application.

**Design Introduction**

**Headquarters (HQ)**
A HQ location is typically a complex network, with high-speed internet links and high availability requirements. In Umbrella, each tunnel is limited to approximately 250mbps per direction. To achieve higher throughput, you will need to establish multiple tunnels. To use multiple tunnels to the best advantage, some means of dividing traffic among tunnels is recommended. These include load sharing with ECMP (Equal-cost multi-path routing) or assigning traffic through policy-based routing. For basic information about ECMP, refer to [RFC 2991](https://www.rfc-editor.org/rfc/rfc2991).

© 2021 Cisco and/or its affiliates. All rights reserved.
HQ network diagram

As the HQ typically contains a larger number of users, SAML integration can be implemented in order to create more granular policies for specific AD users or groups (employees vs. contractor for example). AD users and groups can be provisioned by automatically by using Active Directory-based provisioning with the Umbrella AD Connector. For large networks, having more granular control across specific user groups can be important.

Branch

The Branch is a smaller location with some local network resources that might include local servers and fewer employees. The Branch will consist of:
- An on-premise device capable of connecting an IPsec tunnel to Umbrella
- Policy settings that are unique and different from HQ or corporate security policies
- A single branch identity
- Optional: Cisco SD-WAN technology
- Optional: SAML integration. This configuration will not be replicated in this document. For adding SAML integration to the branch network, refer to the Headquarters Identity configuration.
Roaming

The AnyConnect software is included with the Umbrella SIG Essential package. This includes DNS and SWG protections. VPN functionality is licensed separately. Roaming users are the employees that work remotely from home, on client sites, or use unsecured networks. The Cisco Umbrella Roaming Security module provides always-on security on any network, anywhere, any time—both on and off your corporate VPN. The Roaming Security module consists of two services; Cisco AnyConnect Umbrella Roaming Security Agent and Cisco AnyConnect SWG Agent. The Roaming Security Agent redirects traffic for enforcement at the DNS layer to block malware, phishing, and command and control callbacks over any port. The SWG Agent redirects web traffic to Umbrella for security and visibility.
SIG Deployment

Software versions used in this guide

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ISR</td>
<td>16.06.04</td>
</tr>
<tr>
<td>vManage</td>
<td>20.3.1</td>
</tr>
<tr>
<td>vSmart</td>
<td>20.3.1</td>
</tr>
<tr>
<td>vBond</td>
<td>20.3.1</td>
</tr>
<tr>
<td>vEdge</td>
<td>20.3.1</td>
</tr>
<tr>
<td>AnyConnect</td>
<td>4.9.00086</td>
</tr>
<tr>
<td>Duo Network Gateway</td>
<td>1.5.10</td>
</tr>
<tr>
<td>AD FS Service</td>
<td>10.0.0.0</td>
</tr>
<tr>
<td>Microsoft AD</td>
<td>Windows Server 2016</td>
</tr>
</tbody>
</table>

Before You Start

Step 1. **Plan your policies** – Creating policies, ordering them, and then having them protect your organization and systems exactly how you need them to takes planning and an understanding of how Umbrella’s policies work. It is recommended you read through all of these steps, before beginning policy creation.

Step 2. **Choose your identities** – An identity can be a high-level entity within your system (e.g. a network) or very granular (e.g. a single user). It is important to define how granular the identities will be. Umbrella uses the following identities:

- Network – may be a single public IP address, or a range of public IP addresses
- Network Device – a physical piece of hardware that forwards DNS requests from client computers to Cisco Umbrella
- Roaming Computers – computers protected by either the Umbrella Roaming Client or the Umbrella Roaming Security Module for AnyConnect
- Mobile Devices – devices, such as a phone, traditionally with an Android or iOS operating system. These identities only allow DNS protection when roaming
- Chrome Book – utilize the Cisco Umbrella Chrome Book Client to connect to Umbrella
- Network Tunnel – associated with any traffic flowing over an IPSec tunnel to Umbrella
- Web Users and Groups – associated with SAML user and group objects

Step 3. **Understanding policy behavior** – Policies are evaluated toward an identity starting at the top of the policy list and moving downward until a match is made. Thus, the first identity to match a policy is the policy that is enforced.
**Step 4. Start with the default policy** – For both DNS and Web policies, the Default policy applies to any identity that does not match any other policy. It is the policy of last resort. As such, it is recommended that this becomes the most restrictive policy. Consider using the default policy for the majority of users and devices.

**Step 5. Build additional policies as exceptions, from least specific to most specific** – After configuring Default, you might create additional policies for “All Roaming Computers”, then layer another policy on top of that for a small number of roaming computers that have slightly different requirements.

**Setting up the identities**

**Headquarters (HQ)**

The first step of the deployment is to register a Network identity. A Network identity can be one or more public IPs or an IP range. Registering a Network identity ensures that the specific IP space is correctly assigned to your organization in Umbrella. Depending on the network design, a HQ site may have more than one egress IPs. It is recommended to register all your networks initially to ensure that they're available immediately when you point traffic to Umbrella.

For the HQ site in this deployment, we considered two separate network segments - Employee and Guest networks. When deploying SIG, you have several choices as to how you can send web traffic to Umbrella. We use the following options for the two network segments:

- **Employee network segment** - We will use proxy auto-config (PAC) file setting in browser to redirect the browser traffic to Umbrella’s SWG. PAC file settings are pushed to employee devices using Group Policy Management Console (GPMC).
- **Guest network segment** - We will set up IPSec tunnel from the internet gateway router (ISR4k) to Umbrella data centers.

For details on other available options for sending web traffic to Umbrella, refer to the [Umbrella User Guide](#).

For more granular identity control, we will also implement SAML integration using Active Directory Federation Services (ADFS) as an identity provider. Umbrella supports a range of identity providers, refer to the [Umbrella documentation](#) for more information on SAML integrations. An example configuration with Duo Access Gateway as identity provider is provided in Appendix A of this document.

The pre-requisites to this setup are:

- A valid Cisco Umbrella SIG Essentials subscription or a free SIG trial
- Domain Controller with Active Directory and DNS service already set up and running at the HQ location
- All the HQ employee devices are joined to the AD domain

**Procedure 1. Register the HQ Network**

**Step 1.** Navigate to Deployments > Core Identities > Networks and click **Add**. Provide a meaningful **Network Name** and add the Public egress IP address for HQ site. Click **SAVE** to register the public IP address for the HQ site.
Procedure 2. DNS forwarding to Umbrella

Step 1. From the Start menu on the Windows Server with DNS service, go to DNS Manager. Choose the DNS server and then double click on the Forwarders option to launch properties window. On the Forwarders tab, click Edit button to add the Umbrella resolver IP addresses.

The Umbrella IPv4 addresses are:

- 208.67.222.222
- 208.67.220.220
**Step 2.** Navigate to Admin > API Keys on Umbrella dashboard and click on Add to generate token for Umbrella Network Devices. Copy the token once it is generated.

**Step 3.** Login to the Guest network gateway router (ISR4K- acts as DNS Forwarder for Guest network segment). Follow the Umbrella documentation to add the Umbrella DNS Connector configuration.
Procedure 3 Set up SAML Integration with ADFS

**Step 1.** Log in to the domain controller and go to Manage > Add roles and features from Server Manager Dashboard.

**Step 2.** Follow the Add Roles and Features wizard. Select the Installation type as **Role-based or Feature-based installation**, then click Next.
Step 3. On the Select destination server page, click Select a server from the server pool and click Next.

Step 4. On the Select server roles page, select Active Directory Federation Services and click Next and then Install to begin installation.
Step 5. The wizard displays the installation progress. Once the installation is completed, click on **Configure the federation service on this server** to do the initial configuration for ADFS.

Step 6. A new wizard with **Welcome** page will pop up, select Create the **first federation server in a federation server farm** and click **Next**.
Step 7. On the **Connect to AD DS** page, specify an account with domain administrator rights for the Active Directory domain that the ADFS service will connect to and then click **Next**.

![Server Manager Dashboard](image)

Step 8. On the **Specify Service Properties** page, enter the following details before clicking **Next**:

- Browse to the location of the SSL certificate for ADFS service and import it (you will need to create one if you haven’t already)
- Enter a Federation Service Name. This is the FQDN name that was used to create SSL certificate for ADFS service. Make sure the domain name resolves correctly to the ADFS server IP
- Enter a friendly Federation Service Display Name

![Server Manager Dashboard](image)
Step 9. On the **Specify Service Account** page, select **Use an existing domain user account or group Managed Service Account** and click **Next**.
Step 10. On the Specify Configuration Database page, select Create a database on this server using Windows Internal Database and click Next to Review options.

Step 11. Click Next On the Review options page.
Step 12. On the Pre-requisite Checks page, verify that all prerequisite checks were successfully completed and click Configure.

Step 13. Once the ADFS service is configured successfully, click on Close.
Step 14. Log in to the Umbrella dashboard and navigate to **Deployments > Configuration > SAML Configuration** and click **Add**. Select **ADFS** and click **Next**.

![SAML Configuration](image)

Security Assertion Markup Language (SAML) authentication may be configured for Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) integration, providing individual user and group-based identities for policy enforcement. To complete SAML configuration, access to an Identity Provider (IdP) will be required. For more information, please see our [SAML guides](#). If you instead would like to configure SAML authentication for administrative access to your dashboard, you may configure this under the **Admin** section.

<table>
<thead>
<tr>
<th>SAML Web Proxy Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Provider</strong></td>
</tr>
<tr>
<td>ADFS</td>
</tr>
<tr>
<td>Apsave</td>
</tr>
<tr>
<td>Duo Security</td>
</tr>
<tr>
<td>Okta</td>
</tr>
<tr>
<td>OpenAM</td>
</tr>
<tr>
<td>PingID</td>
</tr>
<tr>
<td>Other</td>
</tr>
</tbody>
</table>

**Select SAML Provider**
Select an identity Provider (IdP) to configure SAML authentication.

**Configure ADFS Metadata**
Configure Umbrella to work with your SAML provider by selecting one of the following two options: uploading the XML Metadata file or filling out required fields for your SSO manually. For more information on how to do this, please see our [SAML setup guides](#).

Select a method:
- XML File Upload
- Manual Configuration

**Download the Umbrella Metadata File**
The file will be required when configuring your SSO for Umbrella.

![Download Metadata](image)

Step 15. Download the **Umbrella Metadata file**. Select **XML File Upload** and click on **Next**.

![XML File Upload](image)
Step 16. Switch back to the ADFS server and launch the ADFS management console. In the ADFS Management window, right-click **Relying Party Trusts** to add a relying party trust. On the **Welcome** page on **Add Relying Party Trust Wizard**, leave the **Claims aware** option selected and click on **Start**.

Step 17. In **Select Data Source** page, choose **Import data about the relying party from a file**. Browse the Umbrella Metadata file downloaded in **Step 15** and click **Next**.

Step 18. Add a meaningful **Display name** and **Notes** for Umbrella and click on **Next**.
Step 19. Select **Permit Everyone** policy on the **Choose Access Control Policy** page and click **Next**.
Step 20. On the Ready to Add Trust page click Next.

Step 21. The replying party trust is added at this point. Click on Close, this will automatically launch Add Transform Claim Rule wizard.
Step 22. In Choose Rule Type page on Add Transform Claim Rule wizard, select Send LDAP Attributes as Claims as the Claim rule template and click Next.

Step 23. In Configure Claim Rule page, do the following and click Next:

- Enter a meaningful Claim rule name.
- From the Attribute Store menu, choose Active Directory.
- Map the LDAP attributes - User-Principal-Name to Outgoing Claim Type - Name ID.

Step 24. Click on Apply to complete the configuration.
Step 25. Download ADFS metadata file by visiting the following URL:

https://<ADFS-Server-Address>/FederationMetadata/2007-06/FederationMetadata.xml

Step 26. Go back to Umbrella dashboard and continue the SAML Web Proxy Configuration Wizard (We switched to ADFS config after Step 15 above). Upload the FederationMetadata.xml file downloaded in Step 25 above and click on Next.

Step 27. Select the Re-Authenticate Users frequency – (Never, Daily, Weekly, or Monthly) and click SAVE.
Step 28. At this point, ADFS SAML integration is fully complete. Click on **TEST CONFIGURATION** to validate the integration.

Step 29. Enter the AD credentials when prompted (employee email address and password) and click on **Sign in**. A successful login confirms proper SAML integration with Umbrella.
Procedure 4. Install AD connector to auto provision users and groups

Step 1. Logon to the Active Directory server and create a new user account on the AD domain. Set the sAMAccountName to OpenDNS_Connector and select Password never expires. Make this new user a member of AD group - Enterprise Read-only Domain Controllers.

Step 2. Switch back to Umbrella dashboard, navigate to Deployments > Configuration > Sites and Active Directory and click Download. Click DOWNLOAD for Windows Configuration script for Domain Controller and Windows Service (Active Directory Connector).

Note: The connector service does not have to be installed on a domain controller. It can be installed on any Windows server that is a member of the domain. For this deployment, we installed it on the HQ domain controller.
Step 3. Login to the domain controller and as an admin user, open an elevated command prompt. From the command prompt, enter: `cscript <filename> --forcenonva true` where `<filename>` is the name of the configuration script you downloaded and copied in Step 2.

![Command Prompt Output](image1)

Step 4. Extract the contents of the ZIP file (OpenDNS-Windows-Service.zip) you downloaded in Step 2. Navigate to the extracted folder to run `Setup.msi`. Umbrella Connector setup wizard is launched, click on **Next** to start the installation.

![Umbrella Connector Setup](image2)
Step 5. Select an install location and then click on Next.

![Destination Folder](image)

Step 6. Enter the Username of the connector user created in Step 1 (OpenDNS_Connector) and the Password. Click on Next.

![Active Directory Credentials](image)

Step 7. Click Next to continue the installation.
Step 8. Click **Install** to begin the installation process.

Step 9. Click **Finish** once the installation is done.
Step 10. Return to the Umbrella dashboard and navigate to **Deployments > Configuration > Sites and Active Directory**. On the **Sites and Active Directory** page, we see the hostname of the domain controller on which the script was run and the connector was installed.

Step 11. Navigate to **Deployments > Core Identities > Web Users and Groups** and click **Users Provisioning**. Select **AD Based Provisioning** and click **Save**. The SAML Users and Groups section appears with the provisioned objects. SAML User and SAML Group identities can be applied to the Web policies now.

**Note:** SAML needs to be enabled in the Web policies for activating end user authentication. Refer to the **Web Policies** section of this document below for more details on enabling SAML authentication.
Procedure 5. Installing Umbrella root CA certificates

Step 1. In Umbrella, navigate to Deployments > Configuration > Root Certificate. Download the Cisco Umbrella root certificate.

Note: You can also add your own CA certificate instead of the Umbrella root CA certificate. Refer to Umbrella documentation for detailed steps.

Step 2. Log in to the domain controller and go to Group Policy Management Console. Select organization level Group Policy Object and right click on it to select Edit option. The Group Policy Management Editor is displayed.

Note: This method of Group Policy based CA certificate push to end users would only work for domain users. For non-domain users and devices, a manual certificate installation might be required. Refer to the Umbrella documentation for detailed information on various methods for CA certificate installation.
Step 3. In the configuration options on sidebar, navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**, right-click on **Trusted Root Certification Authorities**, and select **Import**. Follow the certificate import wizard to import and install the Umbrella root CA certificate in **Trusted Root Certification Authorities** store.

Procedure 6. Set up the PAC file redirection for Employee network

Step 1. Navigate to **Deployments > Configuration > Domain Management** and click on **Add**. Add the FQDN for ADFS server (Identity Provider) under **Domain** and a **Description** for the domain. Use the SAML identity provider FQDN used in **Procedure 3-Step 5**.
Note: Umbrella copies internal domains configured in the Umbrella dashboard to the PAC file so that these internal domains are not sent to the proxy. We need this step to exempt traffic destined to ADFS server (SAML Identity provider) from being forwarded to the Umbrella SWG. This is required to avoid any redirect loop during SAML authentication.

Step 2. In Umbrella, navigate to Policies > Management > Web Policies. Expand Advanced Settings under Default Web Policy and copy the PAC file URL.
Step 3. Login to the Domain Controller and go to Group Policy Management Console. Right click on the organizational OU for HQ employees from the panel on the left hand side and select Create a GPO in this domain, and Link it here. A New GPO window appears. Enter a Name for the new GPO policy and leave Source Starter GPO as (none). Click on OK to save new GPO policy.

Step 4. Right-click on the newly created GPO and select Edit. In the Group Policy Management Editor window, navigate to User Configuration > Preferences > Control Panel Settings > Internet Settings. Right-click on Internet Settings and select Internet Explorer 10. From the Connections tab, click LAN settings. Enter the PAC file URL in the Address field. Click OK.

Note: Browsers such as Microsoft Edge, Google Chrome, and Opera inherit PAC file configuration from Internet Explorer on Windows machines. However, Mozilla Firefox requires a separate configuration. To distribute a PAC file URL to Firefox browsers using GPOs, refer to the Mozilla documentation.

Step 5. To disable automatic configuration for the PAC file settings for end users, navigate to User Configuration > Policies > Administrative Templates > Windows Components > Internet
Explorer. From the Internet Explorer folder, double-click **Disable changing Automatic Configuration** settings. In the pop up window, select **Enabled** and click **OK**.

**Step 6.** On the same window, find **Prevent changing proxy settings** and double-click on it. In the pop up window, select **Enabled** and click **OK**. This will ensure that the end user is not able to change their proxy settings.

**Step 7.** Verify the end user browser proxy settings by navigating to **Internet Settings** > **Connections** tab and clicking on **LAN settings**.
Procedure 7. Set up the IPSec Tunnel for Guest network

Step 1. Navigate to Deployments > Core Identities > Network Tunnels and click on Add to add a tunnel for HQ site. Add a meaningful Tunnel Name, select Device Type as ISR and click on SAVE.

Step 2. Provide a Tunnel ID and Passphrase. Click on SAVE and make sure you copy and keep a note of the tunnel ID and passphrase.

Step 3. To Configure the IPSec tunnel on ISR, we will require the following details.

- Choose an Umbrella DC IP address from the list.
- Tunnel ID and passphrase from the configuration in Step 1.

Login to the ISR router and configure the VPN tunnel, a sample configuration is as below.

Note: Refer to the Umbrella documentation for more details on supported IPSec parameters and cipher configuration.
Cisco ISR tunnel configuration from HQ site (sanitized):

```plaintext
crypto ikev2 proposal umbrella
  encryption aes-gcm-256
  integrity sha256
  group 19 20
!
crypto ikev2 policy umbrella
  proposal umbrella
match address local <INTERNET-FACING-INTERFACE-PUBLICIP>
!
crypto ikev2 keyring umbrella
  peer umbrella
    address <UMBRELLA-DC-IP>
    pre-shared-key <PASSPHRASE>
!
crypto ikev2 profile umbrella
match identity remote addresses 146.112.64.0 255.255.192.0
  identity local email <TUNNEL-ID>
  authentication remote pre-share
  authentication local pre-share
  keyring local umbrella
  dpd 10 2 periodic
!
crypto ipsec transform-set umbrella esp-aes 256 esp-sha-hmac
  mode tunnel
!
crypto ipsec profile umbrella
set transform-set umbrella
set ikev2-profile umbrella
!
interface Tunnel1
  ip unnumbered <INTERNET-FACING-INTERFACE>
  tunnel source <INTERNET-FACING-INTERFACE>
  tunnel mode ipsec ipv4
  tunnel destination <UMBRELLA-DC-IP>
  tunnel protection ipsec profile umbrella
!
ip access-list extended To_Umbrella
  permit ip <LAN-SUBNET> 0.0.0.255 any
!
route-map umbrella-routemap permit 10
  match ip address To_Umbrella
```

© 2021 Cisco and/or its affiliates. All rights reserved.
set interface Tunnel1
!
interface <LAN-INTRFACE>
ip policy route-map umbrella-routemap
!

**Step 4.** Once the configuration is completed, run the command `show crypto session detail` to see the status of the tunnel. The tunnel status will be seen as **UP-ACTIVE** and if there is any active traffic then inbound and outbound packet counters will start incrementing.

![Image of show crypto session detail command output]

**Step 5.** Login to the Umbrella dashboard and navigate to **Deployment > Core Identities > Network Tunnels**, if everything is configured correctly then the **Tunnel Status** will be seen as **Active**.

![Image of Umbrella dashboard with Network Tunnels section]

**Branch**

Direct Internet Access (DIA) is a component of the Cisco SD-WAN architecture in which certain Internet-bound traffic or public cloud traffic from the branch can be routed directly to the Internet, thereby bypassing the latency of tunneling Internet-bound traffic to a central site.

For lab testing purposes, a private SD-WAN environment consisting of vManage, vBond, vSmart and a single vEdge were used following the procedure in the [Cisco SD-WAN End-to-End Deployment Guide](https://www.cisco.com/c/en/us/support/docs/wan/service-provider/731869411065.html). The resulting configuration for each entity can be found in Appendix B. For establishing a tunnel to Umbrella SIG with a device other than vEdge, see [network tunnel configuration](https://www.cisco.com/c/en/us/support/docs/wan/service-provider/731869411065.html). Additionally, an example of building a manual tunnel with a Cisco ISR device can be found in the HQ identity section.

The pre-requisites to this setup are:
vEdge has access to the Umbrella SIG data center public IP addresses, to which the tunnel will connect. For the latest Umbrella SIG DC locations and their IPs, see Cisco Umbrella Data Centers.

All Viptela devices must be running at least version 20.3.1. If using a cEdge device, and, if you require tunnel automation and DNS device integration, use a minimum of version 17.3.1.

An Umbrella organization ID. See Find Your Organization ID

A valid Cisco Umbrella SIG Essentials subscription or a free SIG trial

Allow ports on any upstream device: UDP ports 500 and 4500

The DNS service on the Transport side must be able to resolve management.api.umbrella.com

In a previous section we established that our branch will consist of a single network identity and a network tunnel.

Establish a tunnel between vEdge and Umbrella SIG

Cisco Umbrella auto tunnel support on SD-WAN-enabled WAN Edge routers enables redirection of SIG traffic to the nearest Umbrella Data Center. Auto tunnel supports:

- WAN Edge routers (ISR4K/1K, CSR1000v, ISRv, vEdge)

For all other routers, they must support a security K9 license to establish an IPsec tunnel and must be configured manually. This guide was tested using Viptela 20.3.1. For more tunnel configuration details see Network Tunnel Configuration.

Procedure 1. Enable NAT on vEdge device

Step 1. In vManage, navigate to Configuration > Templates.
Step 1. In the Feature tab, click edit on the VPN 0 interface template (VPN 0 needs WAN connectivity).

Step 2. Click NAT. The screen scrolls to the NAT section.

Step 3. Click the blue arrow (Default), and change to Global. Enable NAT by clicking the On radio button. Update the feature template. If the feature template is attached to a device, follow screen prompts to push updates to the devices.
Procedure 2. Configure SIG template

Step 1. In vManage, navigate to Configuration > Templates > Feature > Add Template.

Step 2. Type vEdge Cloud in the search bar and click to open the template options for vEdge.

Step 3. Under VPN, select Cisco Secure Internet Gateway (SIG).

Step 4. Add a meaningful name to both Template Name and Description.
Step 5. Under Configuration, click Add Tunnel.

   Interface Name: ipsec1
   Source Interface: ge0/0 (for non vEdge devices, refer to documentation for interface name)
   Data-Center: Primary

Step 6. Click add.

Step 7. Create a backup tunnel by repeating steps 5 and 6 with the following.

   Interface Name: ipsec2
   Source Interface: ge0/0
   Data-Center: Secondary
Step 8. Under High Availability, add ipsec1 as active tunnel and ipsec2 as backup tunnel. Click save.

Procedure 3. Configure SIG credentials

Step 1. Take note of your Umbrella organization ID. For a reminder, see Find Your Organization ID.

Step 2. In Umbrella, navigate to Admin > API Keys.

Step 3. If an Umbrella Management API key already exists, take note of the key and secret value. NOTE: the secret will not be displayed, it must be stored somewhere when first created.

Step 4. If an Umbrella Management API key does not exist, click create.
Step 5. Click the Umbrella Management radio button. Click create.

What should this API do? Choose the API that you would like to use.

- Umbrella Network Devices
  Integrate Umbrella-enabled hardware with your organization’s networks. This also enables you to create, update, list, and delete identities in Umbrella.
  - You can only generate one token. Refresh your current token to get a new token.

- Legacy Network Devices
  A Network Devices token enables hardware network devices such as Cisco Wireless Lan Controllers and Cisco Integrated Services Routers 4000 series to integrate with Umbrella.
  - You can only generate one token. Refresh your current token to get a new token.

- Umbrella Reporting
  Enables API access to query for Security Events and traffic to specific Destinations
  - You can only generate one token. Refresh your current token to get a new token.

- Umbrella Management
  Manage organizations, networks, roaming clients and more using the Umbrella Management API

Step 6. Take note of Your Key and Your Secret, check To keep it secure..., and then click close. NOTE: Umbrella will not remind you of Your Secret, so make sure its stored somewhere secure before clicking close.

<table>
<thead>
<tr>
<th>Umbrella Management</th>
<th>Key: f6dc2d51163248c39f487a8ba9e6822f</th>
<th>Created: Oct 1, 2020</th>
</tr>
</thead>
</table>

The API Key and secret pair enable you to manage the deployment for your different organizations. This includes the management of networks, roaming clients and other core-identity types.

Your Key: f6dc2d51163248c39f487a8ba9e6822f

Your Secret: 

To keep it secure, we only display your key’s secret once. For future reference, copy this secret and keep it in a safe place. Tick this box to acknowledge this.

Check out the documentation for step by step instructions.

Step 7. In vManage, navigate to Configuration > Templates > Feature > Add Template.

Step 8. Type vEdge Cloud in the search bar and click to open the template options for vEdge.

Step 9. Under Other Templates, click SIG Credentials.
Step 10. Add a meaningful name to both **Template Name** and **Description**.

Step 11. Enter the **Organization ID**, **Registration Key**, and **Secret** generated in the beginning of this procedure. Click **Save**.
Procedure 4. Attach SIG feature templates to device

**Step 1.** In vManage, navigate to Configuration > Templates > Device and edit the template that belongs to the vEdge you wish to establish a tunnel.

**Step 2.** Under Transport & Management > Additional VPN 0 Templates, click Secure Internet Gateway.

**Step 3.** Click the Secure Internet Gateway drop-down menu and choose the SIG feature template that was created in the previous step.
Step 4. Scroll down to Additional Templates, click SIG Credentials drop-down menu and choose the SIG credentials feature template that was created in the previous step. Click update and push changes to the devices.

Procedure 5. Re-direct traffic through tunnel

This procedure also applies to existing VPN configuration for data traffic that exist on the vEdge. In this example, an assumption has been made that no VPN templates have yet been created to handle data.

Step 1. In vManage, navigate to Configuration > Templates > Feature > Add Template.
Step 2. Under Select Devices, choose vEdge-Cloud.
Step 3. Under VPN, click VPN.
Step 4. Add a meaningful name to both **Template Name** and **Description**.

![Cisco vManage](image)

Step 5. Under **Basic Configuration**, assign a **VPN** value. 1 was used for this test, but any value other than 0 and 512 will work.

![Basic Configuration](image)

Step 6. Ensure **Primary DNS Address (IPv4)** is set to **Default** (blue tick) as DNS redirection has already been setup in previous steps.

![DNS](image)

Step 7. Under **Service Route**, click **New Service Route**.

![Service Route](image)

Step 8. SIG will be chosen by default. Add 0.0.0.0/0 to **Prefix** to route all traffic through SIG. Click **Add**.

![Prefix](image)

Step 9. At bottom of screen, click **Save**.

Step 10. In vManage, navigate to **Configuration > Templates > Feature > Add Template**.

Step 11. Under **Select Devices**, choose **vEdge-Cloud**.

Step 12. Under **VPN**, click **VPN Interface Ethernet**.
Step 13. Add a meaningful name to both Template Name and Description.

Step 14. Under Basic Configuration, set Shutdown to No and provide the devices Interface Name for data traffic. For testing purposes, ge0/2 was used on the vEdge.

Step 15. Staying under Basic Configuration, change IPv4 Address to Device Specific and change the variable name to vpn1_if_ipv4_address (or whatever VPN number you chose).
Step 16. Click Save.

Step 17. In vManage, navigate to Configuration > Templates > Device and edit the vEdge template.

Step 18. Click Service VPN > Add VPN. Select the VPN template from the previous step from the available list to the selected list. Click Next.

Step 19. Click Additional VPN Templates > VPN Interface. Choose the VPN interface template that was created to handle data traffic. Click Add.

Step 20. Click Update.
Step 21. Enter a value for IPv4 Address(vpn1_if_ipv4_address). NOTE: name will differ depending on value entered in step 15. This is the IP address of the routing interface for data traffic. Click next and Configure Devices.

Procedure 6. Check tunnels have been established

Step 1. In Umbrella, navigate to Deployments > Core Identities > Network Tunnels.

Step 2. If tunnels successfully established, you should see both the primary and backup tunnel in an active state.

The tunnel names that are given do have significance. The string consists of the site name, system ip and interface of the device that this tunnel has been established with. To rename these tunnels, continue to step 3.

Step 3. To rename the tunnels, click the ellipsis and choose edit.

Step 4. Update Tunnel Name and click Save.
These tunnels will be used as the identity when creating firewall and web policies for the branch in later sections.

**Adding a network device identity to Umbrella**

For cases in which a tunnel is not desired, a network identity can be added to Umbrella for the matching against DNS policies only. Umbrella does have the capability to send DNS traffic over an IPSec tunnel, however, this example shows how to create the network identity without it.

**Procedure 1. Generate API keys in Umbrella**

**Step 1.** In Umbrella, navigate to Admin > API Keys.
Step 2. If an **Umbrella Network Devices** API key already exists, take note of the key and secret value. 
**NOTE:** the secret will not be displayed, it must be stored somewhere when first created.

Step 3. If an **Umbrella Network Devices** API key does not exist, click create.

Step 4. Click the **Umbrella Network Devices** radio button. Click create.

Step 5. Take note of Your Key and Your Secret, check To keep it secure..., and then click close. 
**NOTE:** Umbrella will not remind you of Your Secret, so make sure its stored somewhere secure before clicking close.
Procedure 2. Configure Cisco Umbrella Registration in vManage

Step 1. In vManage, select Configuration > Security.

Step 1. Click Custom Options and select Umbrella Registration.
Step 2. In the Manage Umbrella Registration dialog box, enter your **Organization ID**, **Registration Key** and **Secret**. Click **save**.

![Manage Umbrella Registration dialog box](image)

**Procedure 3. Optional: Create a domain bypass list**

**Step 1.** In vManage, select **Configuration > Security**.

**Step 2.** Click **Custom Options > Lists**.

![Custom Options with Security lists](image)
Step 3. Click **Domain > New Domain List** to create a new domain list or edit an existing list using the pencil icon on the right side of the entry.

![Image of Cisco vManage interface with New Domain List highlighted](image)

Step 4. Enter the **Domain List Name**, **Add Domain**, and click **Add** to create the list.

![Image of Domain List creation interface in vManage](image)

**Procedure 4. Configure DNS Policy in vManage**

**Step 1.** In vManage, select **Configuration > Security > Add Security Policy**.

![Image of vManage interface showing Security > Add Security Policy](image)
Step 2. Choose Direct Internet Access. Click proceed.

Step 3. Click next until you reach DNS Security tab.

Step 4. Click Add DNS Security Policy and choose Create new.

Step 5. Fill in the required fields and click Save DNS Security Policy.

Enter a meaningful policy name in the Policy Name field.

Check that Umbrella Registration Status has been configured. If not, revisit Procedure 2 above as the details you entered may have been incorrect.

Click Match All VPN radio button.

Add the Local Domain Bypass List from the previous step if applicable. Otherwise leave blank.

Click Advanced tab to enable or disabled DNSCrypt. It is enabled by default.
Step 6.  Click **next** until the policy summary tab. Give the policy a meaningful name and click **Save Policy**.

Procedure 5. Attach DNS Umbrella Policy to Device template

Step 1.  In vManage, select **Configuration > Templates**.
Step 2. In the **Device** tab, edit the vEdge template that attaches to the vEdge(s) you wish to integrate with Umbrella. This template should have been created as part of pre-requisites mentioned earlier.

![Cisco vManage screenshot](image)

Step 3. Click **Additional Templates**. The screen scrolls to the **Additional Templates** section.

Step 4. Click **Security Policy** drop-down list and choose the name of the Umbrella DNS Security Policy you configured above. Click **update** and push policy to devices.

![Cisco vManage Additional Templates screenshot](image)

Step 5. On Umbrella, navigate to **Deployments > Core Identities > Network Devices**. If deployment was successful, the device, and its active VPN's will be shown. This identity is used when creating DNS policies in later sections of this document.

![Cisco Umbrella Deployments screenshot](image)
Step 6. On a the client device that has a route to SIG ping welcome.umbrella.com. A successful response will result in DNS logs appearing in the Umbrella dashboard.

Roaming Computers

For the roaming users on public networks, we have a Cisco ASA running as VPN headend at the HQ site. This guide assumes that roaming users already use Anyconnect VPN mobility client to connect to the HQ site. We will configure the Cisco AnyConnect on the ASA headend to enable Umbrella Roaming Security module. The AnyConnect software is included with the Umbrella SIG Essential package. This includes DNS and SWG protections. VPN functionality is licensed separately.

The AnyConnect Umbrella module installs two agents on the localhost, AnyConnect Umbrella Roaming Security Agent and Cisco AnyConnect SWG Agent. The Roaming Security Agent enforces security at the DNS layer to block malware, phishing, and command and control callbacks over any port. The IP Layer Enforcement feature of Umbrella Roaming agent can also block IP to IP communication. The SWG Agent enforces security at the URL layer, to provide security and visibility for web traffic.
Procedure 1. Anyconnect Roaming Client Settings


Note: Refer to the Umbrella documentation for detailed information Roaming Computer Settings.

Step 2. Switch to Anyconnect Roaming Client tab on the same page, enable Secure Web Gateway option.

Note: SAML is not supported for Roaming users at the time of writing of this guide. To be able to use AD usernames and groups as identities, roaming users must be part of the domain (user information on non-domain and BYOD devices are not reported to the dashboard). The AD connector and script needs to be installed to leverage AD user and group. We already performed this step in a previous section of this document (Setting up the identities > Headquarters > Procedure 4). For more information on identity support for Roaming users, refer to the Umbrella documentation.
Step 3. Navigate to Deployments > Roaming Computers and click on Roaming Client on the top right hand side. Under AnyConnect Umbrella Roaming Security Module, click Download Module Profile to download the OrgInfo.json file. Move this file to the VPN headend ASA’s flash drive.
Procedure 2. Update the ASA Configuration

Step 1. Log in to the ASDM and navigate to Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile and click on Add. Map the OrgInfo.json profile to roaming user’s Group Policy.

Step 2. Navigate to Configuration > Remote Access VPN > Network (Client) Access > Group Policy and select the roaming user’s group policy, add the text umbrella under Optional Client Modules to Download. Under Client Profiles to Download, make sure that the Umbrella profile that we created in Step 1 shows up. Save the changes on ASA.

Cisco ASA Anyconnect Roaming Client configuration from HQ site:
webvpn

    anyconnect profiles roaminguser-umbrella disk0:/OrgInfo.json

!
group-policy roaminguser_policy attributes

webvpn

    anyconnect modules value umbrella
    anyconnect profiles value roaminguser-umbrella type umbrella

!

Procedure 3. Verify the Roaming user status

Step 1. Launch the Anyconnect VPN client and connect to the VPN headend. End user will be provisioned with the newly set up Umbrella Roaming client. Disconnect after the successful install and connection.

Step 2. Roaming Security module shows ‘Umbrella is active’. Click on the gear icon icon and select Roaming Security option from the sidebar. Message History tab shows the connection events. The event log “You are protected by secure web gateway” confirms that the roaming user is properly set up.

Step 3. Navigate to Deployments > Roaming Computers. The newly registered roaming user should show up in the list. Click on the Identity Name to see the detailed configuration for a specific user.
DNS Policies

Setting up the policies

**Step 1.** Navigate to **Policies > Management > DNS Policies** and click **Add**.

**Step 2.** Disable **Access Control > Application control** for DNS policies. Application control requires SSL inspection to be enabled, which for a SIG deployment will be covered in web policies and should not be duplicated here. The only thing kept active is the Security Category Blocking, which blocks access to malicious domains. Selecting an option here makes that component available for configuration in the Policy wizard’s later steps.
How would you like to be protected?
Choose which type of access control or threats to block. Your selection will determine what features are available to the policy, what level of visibility is provided in your reports, and should match how Umbrella is deployed in your environment. For more information, click here.

Select Your Protection:

- **Access Control**
  Restrict access with broad category based blocking and/or surgical block and allow destination lists.
  - **Content Category Blocking**
    Block access to destinations based on content category.
  - **Apply Destination Lists**
    Create or modify lists to explicitly block or allow destinations. Note: global block and global allow destination lists are applied by default.
  - **Application Control**
    Block or allow access to applications individually or by group.

- **Block Threats**
  Secure your network and endpoints using a variety of antimalware engines and threat intelligence.
  - **Security Category Blocking**
    Ensure domains are blocked when they host malware, command and control, phishing, and more.
  - **File Analysis**
    Inspect files for malware using signatures, heuristics and file reputation (powered by Cisco Advanced Malware Protection).
  - **IP-Layer Enforcement**
    Block threats that bypass DNS lookups by tunneling suspect IP connections. Note: this is only available for roaming computer identities.

**Advanced Settings**

---

**Step 3.** Expand **Advanced Settings**, **disable** the intelligent proxy and click **next**. For SIG deployments, the intelligent proxy is disabled as this module is separate from the web proxy.

**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.
  - **Enable IP-Layer Enforcement**
    Gain visibility into threats that bypass DNS lookups by tunneling suspect IP connections. Note: this is only available for Roaming Computer identities.

**Note:** When creating a policy you may come across a screen (see below) that does not allow you to toggle the intelligent proxy in this step. If this occurs, disable the intelligent proxy at the very last step of policy creation, during the summary screen.
Step 4. Choose the identities to be protected. Top-level groups like “All networks” and “All Roaming Computers” are special because they dynamically inherit new identities. It is recommended to utilize these top level identities, and create more granular control using firewall and web policies. Click next.

Step 5. Under the Select Setting drop-down, click add new setting. Any changes made to the default setting will result in new policies inheriting the changes and leaves room for error. Make sure to give a meaningful name to the policy for easy referencing.
Step 6. Choose the categories to block using DNS. It is recommended to enable all of these by default for maximum protections.
Step 7. Click next on the block page settings unless you have reason to change the default. To create a custom block page see customize block pages.

Set Block Page Settings

Define the appearance and bypass options for your block pages.

- Use Umbrella’s Default Appearance
  - Preview Block Page

- Use a Custom Appearance
  - Choose an existing appearance

Step 8. Assign a Policy Name, verify the settings (ensure intelligent proxy is disabled), and click save.

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Protection</th>
<th>Applied To</th>
<th>Contains</th>
<th>Last Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIG Policy</td>
<td>DNS Policy</td>
<td>1 Identity</td>
<td>2 Policy Settings</td>
<td>Oct 1, 2020</td>
</tr>
</tbody>
</table>

- 1 Identity Affected
  - 1 Network Device
    - Edit Identity

- Security Setting Applied: SIG DNS
  - Command and Control Callbacks, Malware, Phishing Attacks, plus 5 more will be blocked
  - No integration is enabled.
    - Edit
    - Disable

- No Content Settings Applied
  - Enable

- No Application Settings Applied
  - Enable

- 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.
    - Enable IP-Layer Enforcement
      - Gain visibility into threats that bypass DNS lookups by tunneling suspect IP connections. Note: this is only available for Roaming Computer identities.
Step 9. Test the policy. On a client device that will be assigned to the identity created in the policy above, navigate to any web page in the browser. For the purposes of this test, a Ubuntu device was used, connected to SIG via the vedge router in the branch network. In Umbrella, navigate to Reporting > Core Reports > Activity Search. If the policy was assigned correctly, and logging was enabled, all DNS traffic from that identity will be reported here.

Firewall Policies

Step 1. Navigate to Policies > Management > Firewall Policies and click on Add to add rules for filtering TCP/UDP/ICMP traffic sourcing from HQ and Branch locations.

Step 2. Provide a name and priority for the rule. For lab validation purposes, we are denying the DNS traffic to all other providers except Cisco Umbrella Resolvers.
**Step 3.** Firewall policies will be processed from top to bottom against the traffic incoming from various sources, only the DNS traffic destined to Umbrella resolvers will be allowed.

**Web Policies**

**Step 1.** Navigate to Policies > Management > Web Policies and click Add.
Step 2. Choose which type of access control or threats to block. It is recommended to leave as default to take advantage of all available features.

How would you like to be protected?
Choose which type of access control or threats to block. Your selection will determine what features are available to the policy, what level of visibility is provided in your reports, and should match how Umbrella is deployed in your environment. For more information, click here.

Select Your Protection:

- **Access Control**
  - Restrict access with broad category based blocking and/or surgical block and allow destination lists.
    - **Content Category Blocking**
      - Block access to destinations based on content category.
    - **Apply Destination Lists**
      - Create or modify lists to explicitly block or allow destinations. Note: global block and global allow destination lists are applied by default.
  - **Application Control**
    - Block or allow access to applications individually or by group.
  - **File Type Control**
    - Block file downloads by file type.
  - **Tenant Controls**
    - Allow user access to enterprise approved cloud apps or suites, while blocking all personal or otherwise unwanted use.

- **Block Threats**
  - Secure your network and endpoints using a variety of antimalware engines and threat intelligence.
    - **Security Category Blocking**
      - Ensure domains are blocked when they host malware, command and control, phishing, and more.
    - **File Analysis**
      - Inspect files for malware using signatures, heuristics and file reputation (powered by Cisco Advanced Malware Protection).
    - **IP-Layer Enforcement**

Advanced Settings
Step 3. Optional; Click **Enable SAML** authentication under **Advanced Settings** if you plan on applying policy to groups within a top level network or tunnel identity. Click **next**. For more information on SAML configuration refer back to the HQ identity section.

Advanced Settings
Please read our deployment guide for configuring your environment to use a PAC file or proxy chaining, [here.](#)

**PAC file URL**  https://proxy.prod.pac.swg.umbrella.com/22182269a885f59790b4cbbd9de96ad9f/proxy.pac

Note: PAC file downloads and usage are limited to fixed networks registered in Umbrella. PAC files are not supported for roaming computers or other connection mechanisms.

- **Enable SAML**
  Enables SAML authentication on the networks and tunnels configured in this policy.

LOGGING

- **Log All Requests**
- **Log Only Security Events**
  Log and report on only those requests that match a security filter or integration, with no reporting on other requests.
- **Don’t Log Any Requests**
  Note: No requests will be reported or alerted on. Unreported events will still be logged anonymously and aggregated for research and threat intelligence purposes.

Step 4. Choose the identity to apply this policy to. Refer back to the **Before You Start** section on best practices here. Click **next**.

What would you like to protect?

<table>
<thead>
<tr>
<th>Select Identities</th>
<th>All Identities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Identities</td>
<td>Networks 2</td>
</tr>
<tr>
<td></td>
<td>Roaming Computers 2</td>
</tr>
<tr>
<td></td>
<td>Groups 9</td>
</tr>
<tr>
<td></td>
<td>Users 5</td>
</tr>
<tr>
<td></td>
<td>Tunnels 1</td>
</tr>
</tbody>
</table>

2 Selected

| REMOVE ALL |
| Networks 2 |

CANCEL  PREVIOUS  NEXT
Step 5. **Enable** HTTPS inspection for maximum protection. Umbrella uses **Cisco Talos** web reputation plus other third-party feeds to determine if a URL is malicious. If it is not and there is no other administrative block configured in the Web policy that the URL would match - Umbrella SWG retrieves the requested content from the webserver and scans it using an anti-virus (AV) engine including Cisco AMP file reputation. Additionally, HTTPS inspection must be enabled to enforce application settings and file type control. You must also install a CA root certificate in all browsers. For more information, see **manage certificates**.

HTTPS Inspection
Configure how Umbrella should handle HTTPS traffic. See HTTPS Inspection

- **Enable HTTPS Inspection**
  HTTPS traffic is intercepted and decrypted to provide security and policy enforcement at the URL layer, and visibility into the URL path. By default, HTTPS inspection attempts to decrypt all HTTPS traffic. For any HTTPS traffic that should not be decrypted, create a bypass inspection group.

Add domains and select categories you want to exempt from HTTPS inspection:

- **None**
- **0 Categories Selected**
- **0 Domains**

- **Install Root Certificate**
  Without a certificate installed, users will not be able to connect to some HTTPS sites and SSL connections could be broken. Your root certificates are available under Deployments > Configuration > Root Certificates. View Distributing Root Certificates

- **Decrypt Blocked Traffic Only**
  Enable this feature for policies that should not inspect HTTPS traffic, but where HTTPS block pages are required.

- **Disable HTTPS Inspection**
  HTTPS traffic is not intercepted. Domain layer security and policy enforcement still apply, and only domain layer visibility is possible.

**Step 6.** Optional: Add selective decryption. Categories selected in this list will not undergo SSL decryption. Umbrella provides popular options to enable. A full list can be found in step 11 below. Click **next** on HTTPS inspection page.
Step 7. Click next to continue with the default security settings. All traffic that falls into these categories will be enforced through the web proxy.

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 Web Settings
**Step 8.** Choose which application content will be restricted. By default, Umbrella policy enforcement works on the principle of implicit allow. Meaning, if something is not explicitly blocked, such as a security threat category match or a destination block list match, Umbrella allows the transaction.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Academic Fraud</td>
<td>File Storage</td>
<td>Mobile Phones</td>
<td>Research / Reference</td>
</tr>
<tr>
<td>Adult</td>
<td>File Transfer Services</td>
<td>Nature</td>
<td>Saas and B2B</td>
</tr>
<tr>
<td>Alcohol</td>
<td>Financial Institutions</td>
<td>News / Media</td>
<td>Safe for Kids</td>
</tr>
<tr>
<td>Arts</td>
<td>Fireware and Shareware</td>
<td>Non-Profits</td>
<td>Science and Technology</td>
</tr>
<tr>
<td>Astrology</td>
<td>Gambling</td>
<td>Nudity</td>
<td>Search Engines and Portals</td>
</tr>
<tr>
<td>Auctions</td>
<td>Government</td>
<td>Online Communities</td>
<td>Sex Education</td>
</tr>
<tr>
<td>Automotive</td>
<td>Hacking</td>
<td>Online Meetings</td>
<td>Social Networking</td>
</tr>
<tr>
<td>Business Services</td>
<td>Hate / Discrimination</td>
<td>Online Trading</td>
<td>Social Science</td>
</tr>
<tr>
<td>Chat and instant Messaging</td>
<td>Health and Fitness</td>
<td>Organizational Email</td>
<td>Society and Culture</td>
</tr>
<tr>
<td>Child Abuse Content</td>
<td>Humor</td>
<td>P2P / File sharing</td>
<td>Software Updates</td>
</tr>
<tr>
<td>Computer Security</td>
<td>Hunting</td>
<td>Paranormal</td>
<td>Software / Technology</td>
</tr>
<tr>
<td>Dating</td>
<td>Illegal Activities</td>
<td>Parked Domains</td>
<td>Sports</td>
</tr>
<tr>
<td>Digital Postcards</td>
<td>Illegal Downloads</td>
<td>Personal Sites</td>
<td>Streaming Audio</td>
</tr>
<tr>
<td>Drinking and Drinking</td>
<td>Infrastructure</td>
<td>Personal VPN</td>
<td>Streaming Videos</td>
</tr>
<tr>
<td>DIY Projects</td>
<td>Internet Telephony</td>
<td>Photo Search and Images</td>
<td>Testosterone</td>
</tr>
<tr>
<td>Drugs</td>
<td>IT-ADM</td>
<td>Politics</td>
<td>Tobacco</td>
</tr>
<tr>
<td>Dynamic and Residential</td>
<td>IT-AGCOM</td>
<td>Pornography</td>
<td>Travel</td>
</tr>
<tr>
<td>Ecommerce / Shopping</td>
<td>Jobs / Employment</td>
<td>Professional Networking</td>
<td>Weapons</td>
</tr>
<tr>
<td>Educational Institutions</td>
<td>Lingerie / Bikini</td>
<td>Proxy / Anonymizer</td>
<td>Web Hosting</td>
</tr>
<tr>
<td>Entertainment</td>
<td>Lottery</td>
<td>Real Estate</td>
<td>Web Page Translation</td>
</tr>
<tr>
<td>Fashion</td>
<td></td>
<td>Religious</td>
<td>Webmail</td>
</tr>
</tbody>
</table>

Tick the categories which your organization would like to block and click **next**. More information on each category can be found [here](#).

**Step 9.** Configure Umbrella to allow identity access to only approved SaaS applications in the cloud. An example configuration for tenant control usage can be found in appendix C. For more information see [tenant controls](#). Click **next**.
Step 10. Select specific applications you would like to block. This feature could be used to override a block action from a content category. For example, all social media is blocked by the content category, but your organization would like to open the use of Facebook. If deviating from default, make sure to add a new setting and give it a reasonable name. Click save, and next.
Step 11. Add a custom domain list to block if desired and click next. By default we will leave blank. To add a custom list see destination lists.
Step 12. **Enable File inspection.** When File Inspection is enabled, Umbrella inspects inbound files for malware using anti-virus signatures and Advanced Malware Protection (AMP) file reputation before files are downloaded.

**File Analysis**

Inspect files for malicious behaviors using a combination of static and dynamic analysis methods, in addition to file reputation and advanced heuristics.

- **File Inspection**
  - Inspect files for malware using signatures, heuristics and file reputation (powered by Cisco Advanced Malware Protection).

- **Threat Grid Malware Analysis**
  - Analyze files for malicious behavior using advanced sandboxing with static and dynamic threat intelligence

Step 13. Optional: **Enable Threat Grid.** When Threat Grid Malware Analysis is enabled, files not blocked through File Inspection and that are unknown to AMP file reputation may be submitted by Umbrella to Threat Grid for malware analysis. This includes file types known to carry malware or be a conduit for malware, such as EXE and PDF files. For more information on Cisco Threat Grid integration see [manage file analysis](#).

Step 14. **Choose file types to block.** File Type Control enables you to block identities from downloading specific file types. Users that attempt to download file types blocked by a policy will receive a [block page](#) and be unable to download the file. This file control is separate from the AMP reputation list. AMP blocks specific files based on threat reputation, file control policies will block all files of a specified type, regardless of reputation. For more information go to [managing file type control](#). By default we will leave blank since AMP is already blocking files based on Talos threat intelligence, however, to see an example of file type control go to appendix D. Click [next](#).
Edit File Type Control

Choose the file types you would like to block.

Search file types

<table>
<thead>
<tr>
<th>All Groups</th>
<th>0 Selected File Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio</td>
<td>11</td>
</tr>
<tr>
<td>Compressed files</td>
<td>12</td>
</tr>
<tr>
<td>Data and database</td>
<td>11</td>
</tr>
<tr>
<td>Disc and media files</td>
<td>4</td>
</tr>
<tr>
<td>Documents</td>
<td>9</td>
</tr>
<tr>
<td>Executables</td>
<td>22</td>
</tr>
<tr>
<td>Images</td>
<td>12</td>
</tr>
<tr>
<td>System related files</td>
<td>11</td>
</tr>
<tr>
<td>Videos</td>
<td>15</td>
</tr>
</tbody>
</table>

CANCEL  PREVIOUS  NEXT
Step 15. Set block page appearance. Umbrella has its own default block page, although a custom page can be added to match your organization. To add a custom block page, see customizing block pages. Click next.

Set Block Page Settings
Define the appearance and bypass options for your block pages.

- Use Umbrella’s Default Appearance
- Use a Custom Appearance

Choose an existing appearance

The Cisco Umbrella root certificate must be installed on all computers in order to show the selected block page. We only decrypt traffic that is blocked and this is not total traffic inspection.

Step 16. Add a meaningful name to the policy and click save.

Policy Summary

Policy Name

SIG_CVD_WebPolicy

Step 17. Test the policy. On a client device that will be assigned to the identity created in the policy above, navigate Facebook (or any page that you may have blocked in your policy creation). For the purposes of this test, a Ubuntu device was used, connected to SIG via the vedge router in the branch network. In Umbrella, navigate to Reporting > Core Reports > Activity Search. If the policy was assigned correctly, and logging was enabled, all web traffic from that identity will be reported here.
Appendix

Appendix A: Duo Access Gateway for SAML Configuration

This section provides steps for configuring SAML Identities with Duo Access Gateway as Identity Provider.

**Step 1.** Follow the Duo documentation for initial installation of Duo Access Gateway. After the initial installation, log into the Duo Access Gateway portal (displaying the welcome message).

![Duo Access Gateway Welcome Page](image)

**Note:** Note down the Duo Access Gateway (SAML identity Provider) IP address and FQDN. We will need it to exempt traffic destined to Identity provider IP address from being forwarded to Umbrella Secure Web Gateway. This is required to avoid any redirect loop during SAML authentication.

**Step 2.** In the Duo Access Gateway admin console, click on **Authentication Source**. Select the **Active Directory** as **Source type** under **Configure Sources** section. Fill in the LDAP details for the active directory server at HQ location. Follow the Duo documentation for detailed description on each of the prompted AD details. Click on **Save settings** to complete the **LDAP bind** process.
Step 3. On the same Authentication Source page, under Set Active Source section at the top, select Active Directory from drop down menu and click on Set Active Source.

Step 4. Switch to the Duo cloud admin panel, navigate to Policies and click on New Policy under Custom Policies. Enter a Policy Name, select allow access without 2FA and click Create Policy button.
Step 5. Now navigate to Applications. Click on Protect an Application and search for Generic Service Provider – Duo Access Gateway. Add the following SAML service provider (Umbrella) details.

- Service provider name – Any meaningful name
- Entity ID – saml.gateway.id.swg.umbrella.com
Step 6. Scroll down and update Application policy under Policy section to point to custom policy that we created in Step 4 (BypassMFA) to allow access without MFA. After adding the bypass policy, click on Save configuration button.

Note: Follow the Duo documentation for further details on other options available for customizing the SAML behavior.
Step 7. After saving changes, click on Download your configuration file option to download the Duo JSON configuration file. Copy this file to Duo Access Gateway.

![Configure SAML Service Provider](image)

Step 8. Go back to Duo Access Gateway’s console, click on Applications. In the Add Application section of the page and Browse the JSON configuration file downloaded and copied in Step 7. Click the Upload button after selecting the JSON file to finish adding the application.

![Applications](image)

Step 9. After adding the application, click on Download XML metadata to download XML configuration.
Step 10. Log into the Umbrella, navigate to Deployments > Configuration > SAML Configuration and click on Add. Select Duo Security, click on Next.

You have not added SAML configurations yet.
You may add a new SAML configuration by clicking "Add" from the header above.

Step 11. Select XML File Upload. You can download Umbrella metadata file and then click Next (We won’t need this file since we already manually added the Umbrella’s SAML service provider details in Step 5 in this section).
Step 12. On the **Upload Metadata** step, upload the XML metadata file we downloaded in Step 9. Click on **Next** to complete the SAML integration.

![Upload Metadata](image)

Step 13. From the **Re-Authenticate Users** drop-down list, choose how often Umbrella re-authenticates users: **Never, Daily, Weekly, or Monthly** and click **SAVE**. SAML integration is completed at this point.

![SAML Configuration](image)

Step 14. Click on **TEST CONFIGURATION** to verify the integration. Enter the AD credentials when prompted (employee email address and password) and click on **Log in**. A successful login confirms proper SAML integration with Umbrella.

![Log in](image)

**Appendix B: Viptela Configuration Template Summary**

For convenience, this section summarizes the configuratons used for the SD-WAN network, including the feature templates, device templates, and variable values for the SD-WAN devices in the example network. The configuration shows elements that were added to the default. When performing a ‘sh run’ on the device, you may encounter more configuration elements such as ‘logging’ or ‘AAA’, however, that was left as default and it has been decided to only include the relevant configuration in this document.
vManage

system
  host-name        vmanage
  system-ip       1.1.1.1
  site-id         255
  sp-organization-name SBG
  organization-name SBG
  vbond 10.0.0.2
  ntp
    server 10.16.255.1
      vpn 512
  version 4
  exit
!
!
vpn 0
  interface eth1
    ip address 10.0.0.1/24
  tunnel-interface
    allow-service dhcp
    allow-service dns
    allow-service icmp
    no allow-service sshd
    no allow-service netconf
    no allow-service ntp
    no allow-service stun
    allow-service https
  !
  no shutdown
!
vpn 512
  interface eth0
    ip address 10.30.1.51/24
    no shutdown
!
  ip route 0.0.0.0/0 10.30.1.1

vBond

system
  host-name        vbond
  system-ip       1.1.1.2
site-id 255
organization-name SBG
upgrade-confirm 15
vbond 10.0.0.2 local vbond-only!

security
ipsec
  authentication-type ah-shal-hmac shal-hmac
!
!
vpn 0
  interface ge0/0
    ip address 10.0.0.2/24
    ipv6 dhcp-client
tunnel-interface
    encapsulation ipsec
    no allow-service bgp
    allow-service dhcp
    allow-service dns
    allow-service icmp
    no allow-service sshd
    no allow-service netconf
    no allow-service ntp
    no allow-service ospf
    no allow-service stun
    allow-service https
    !
    no shutdown
    !

vpn 512
  interface eth0
    ip address 10.30.1.52/24
    ipv6 dhcp-client
    no shutdown
    !
    ip route 0.0.0.0/0 10.30.1.1
    !

vSmart

system
  host-name vsmart
  system-ip 1.1.1.3
site-id 255
organization-name SBG
upgrade-confirm 15
vbond 10.0.0.2
!
vpn 0
    interface eth1
        ip address 10.0.0.3/24
tunnel-interface
    allow-service dhcp
    allow-service dns
    allow-service icmp
    no allow-service sshd
    no allow-service netconf
    no allow-service ntp
    no allow-service stun
!
    no shutdown
!
!
vpn 512
    interface eth0
        ip address 10.30.1.53/24
        no shutdown
!
        ip route 0.0.0.0/0 10.30.1.1
!
**vEdge**

**Feature Templates**

**System**

Template Name: system_template_vedge

Description: system_template_vedge

<table>
<thead>
<tr>
<th>Section</th>
<th>Parameter</th>
<th>Type</th>
<th>Variable/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Configuration</strong></td>
<td>Site ID</td>
<td>Global</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>System IP</td>
<td>Device Specific</td>
<td>system_system_ip</td>
</tr>
<tr>
<td></td>
<td>Hostname</td>
<td>Device Specific</td>
<td>system_host_name</td>
</tr>
<tr>
<td></td>
<td>Console Baud Rate (bps)</td>
<td>Global</td>
<td>9600</td>
</tr>
</tbody>
</table>

**VPN 0**
Template Name: vpn0_template_vedge
Description: vpn0_template_vedge

<table>
<thead>
<tr>
<th>Section</th>
<th>Parameter</th>
<th>Type</th>
<th>Variable/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Configuration</td>
<td>VPN</td>
<td>Global</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>Global</td>
<td>vpn0</td>
</tr>
<tr>
<td>DNS</td>
<td>Primary DNS Address</td>
<td>Default</td>
<td>-</td>
</tr>
<tr>
<td>IPv4 Route</td>
<td>Prefix</td>
<td>Global</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>Gateway</td>
<td>Radio Button</td>
<td>Next Hop</td>
</tr>
<tr>
<td></td>
<td>Next Hop</td>
<td>Global</td>
<td>10.0.0.254</td>
</tr>
</tbody>
</table>

VPN 0 Interface

Template Name: vpn0_interface_template_vedge
Description: vpn0_interface_template_vedge

<table>
<thead>
<tr>
<th>Section</th>
<th>Parameter</th>
<th>Type</th>
<th>Variable/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Configuration</td>
<td>Shutdown</td>
<td>Global</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Interface Name</td>
<td>Device Specific</td>
<td>vpn0_if_name</td>
</tr>
<tr>
<td></td>
<td>IPv4</td>
<td>Radio Button</td>
<td>Static</td>
</tr>
<tr>
<td></td>
<td>IPv4 Address</td>
<td>Device Specific</td>
<td>vpn0_if_ip4_address</td>
</tr>
<tr>
<td>Tunnel</td>
<td>Tunnel Interface</td>
<td>Global</td>
<td>On</td>
</tr>
<tr>
<td></td>
<td>Color</td>
<td>Global</td>
<td>private1</td>
</tr>
<tr>
<td>NAT</td>
<td>NAT</td>
<td>Global</td>
<td>On</td>
</tr>
</tbody>
</table>

VPN 512

Template Name: vpn512_template_vedge
Description: vpn512_template_vedge

<table>
<thead>
<tr>
<th>Section</th>
<th>Parameter</th>
<th>Type</th>
<th>Variable/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Configuration</td>
<td>VPN</td>
<td>Global</td>
<td>512</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>Global</td>
<td>vpn512</td>
</tr>
<tr>
<td>DNS</td>
<td>Primary DNS Address</td>
<td>Default</td>
<td>-</td>
</tr>
</tbody>
</table>

VPN 512 Interface

Template Name: vpn512_interface_template_vedge
Description: vpn512_interface_template_vedge
<table>
<thead>
<tr>
<th>Section</th>
<th>Parameter</th>
<th>Type</th>
<th>Variable/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Configuration</td>
<td>Shutdown</td>
<td>Global</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Interface Name</td>
<td>Device Specific</td>
<td>vpn512_if_name</td>
</tr>
<tr>
<td></td>
<td>IPv4</td>
<td>Radio Button</td>
<td>Static</td>
</tr>
<tr>
<td></td>
<td>IPv4 Address</td>
<td>Device Specific</td>
<td>vpn512_if_ip4_address</td>
</tr>
</tbody>
</table>

### VPN 1

**Template Name:** vpn1_template_vedge  
**Description:** vpn1_template_vedge

<table>
<thead>
<tr>
<th>Section</th>
<th>Parameter</th>
<th>Type</th>
<th>Variable/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Configuration</td>
<td>VPN</td>
<td>Global</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>Default</td>
<td>-</td>
</tr>
<tr>
<td>DNS</td>
<td>Primary DNS Address</td>
<td>Default</td>
<td>-</td>
</tr>
<tr>
<td>Service Route</td>
<td>Prefix</td>
<td>Global</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>Service</td>
<td>Default</td>
<td>SIG</td>
</tr>
</tbody>
</table>

### VPN 1 Interface

**Template Name:** vpn1_interface_template_vedge  
**Description:** vpn1_interface_template_vedge

<table>
<thead>
<tr>
<th>Section</th>
<th>Parameter</th>
<th>Type</th>
<th>Variable/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Configuration</td>
<td>Shutdown</td>
<td>Global</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Interface Name</td>
<td>Global</td>
<td>ge0/2</td>
</tr>
<tr>
<td></td>
<td>IPv4</td>
<td>Radio Button</td>
<td>Static</td>
</tr>
<tr>
<td></td>
<td>IPv4 Address</td>
<td>Device Specific</td>
<td>vpn1_if_ip4_address</td>
</tr>
</tbody>
</table>

### Umbrella SIG

**Template Name:** umbrella_sig_template_vedge  
**Description:** umbrella_sig_template_vedge

<table>
<thead>
<tr>
<th>Section</th>
<th>Parameter</th>
<th>Type</th>
<th>Variable/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>SIG Provider</td>
<td>Radio Button</td>
<td>Umbrella</td>
</tr>
<tr>
<td>Configuration – Add Tunnel</td>
<td>Tunnel Name</td>
<td>Global</td>
<td>ipsec1</td>
</tr>
<tr>
<td></td>
<td>Source Interface</td>
<td>Global</td>
<td>ge0/0</td>
</tr>
<tr>
<td>Section</td>
<td>Parameter</td>
<td>Type</td>
<td>Variable/Value</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------</td>
<td>----------</td>
<td>----------------</td>
</tr>
<tr>
<td>Configuration – Add Tunnel</td>
<td>Tunnel Name</td>
<td>Global</td>
<td>ipsec2</td>
</tr>
<tr>
<td></td>
<td>Source Interface</td>
<td>Global</td>
<td>ge0/0</td>
</tr>
<tr>
<td>SIG Tunnel Data Center</td>
<td>Global</td>
<td>Primary</td>
<td></td>
</tr>
</tbody>
</table>
### High Availability

<table>
<thead>
<tr>
<th>Section</th>
<th>Parameter</th>
<th>Type</th>
<th>Variable/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Global</td>
<td>ipsec1</td>
<td></td>
</tr>
<tr>
<td>Backup</td>
<td>Global</td>
<td>ipsec2</td>
<td></td>
</tr>
</tbody>
</table>

### Umbrella SIG Credentials

**Template Name:** umbrella_sig_credentials_vedge

**Description:** umbrella_sig_credentials_vedge

<table>
<thead>
<tr>
<th>Section</th>
<th>Parameter</th>
<th>Type</th>
<th>Variable/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Details</td>
<td>SIG Provider</td>
<td>Radio Button</td>
<td>Umbrella</td>
</tr>
<tr>
<td></td>
<td>Organization ID</td>
<td>Global</td>
<td>&lt;ORGID&gt;</td>
</tr>
<tr>
<td></td>
<td>Registration Key</td>
<td>Global</td>
<td>&lt;REGISTRATION KEY&gt;</td>
</tr>
<tr>
<td></td>
<td>Secret</td>
<td>Global</td>
<td>&lt;SECRET&gt;</td>
</tr>
</tbody>
</table>

### Device Templates

#### vEdge Cloud

**Template Name:** vedge_device_template

**Description:** vedge_device_template

<table>
<thead>
<tr>
<th>Section</th>
<th>Template Type</th>
<th>Template Sub-Type</th>
<th>Template Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Information</td>
<td>System</td>
<td></td>
<td>system_template_vedge</td>
</tr>
<tr>
<td>Transport &amp; Management</td>
<td>VPN 0</td>
<td>Secure Internet Gateway</td>
<td>umbrella_sig_template_vedge</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VPN Interface</td>
<td>vpn0_interface_template_vedge</td>
</tr>
<tr>
<td></td>
<td>VPN 512</td>
<td>VPN Interface</td>
<td>vpn512_interface_vedge</td>
</tr>
<tr>
<td>Service VPN</td>
<td>Add VPN</td>
<td>VPN</td>
<td>vpn1_template_vedge</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VPN interface</td>
<td>vpn1_interface_template_vedge</td>
</tr>
<tr>
<td>Additional Templates</td>
<td>Security Policy</td>
<td></td>
<td>sig_test_policy</td>
</tr>
<tr>
<td></td>
<td>SIG Credentials</td>
<td></td>
<td>umbrella_sig_credentials_vedge</td>
</tr>
</tbody>
</table>
CLI Configuration

system
host-name vedge
system-ip 3.1.1.1
site-id 1
admin-tech-on-failure
no route-consistency-check
sp-organization-name SBG
organization-name SBG
console-baud-rate 9600
vbond 10.0.0.2
security
ipsec
  authentication-type sha1-hmac ah-sha1-hmac
!
umbrella
  orgid 2218226
  api-key 648c3ced1fe24e6fb303eff04380b968
  secret 0 c6fe4973defc41bf8b50ebdaa774c03f
dnscrypt
!

secure-internet-gateway
  umbrella org-id 2218226
  umbrella api-key 95a28aa685c7495f9d8d2abc1c9f9626
  umbrella api-secret 89da7a27288e4052b5d15c0ebe0beb6d
!
vpn 0
  name vpn0
  service sig
    ha-pairs interface-pair ipsec1 active-interface-weight 1 ipsec2
      backup-interface-weight 1
    exit
  exit
interface ge0/0
  ip address 10.0.0.11/24
  nat
  !
tunnel-interface
  encapsulation ipsec
color private1
  no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
!
no shutdown
!
interface ipsec1
  ip unnumbered
tunnel-source-interface ge0/0
tunnel-destination dynamic
tunnel-set secure-internet-gateway-umbrella
tunnel-dc-preference primary-dc
ike
  version 2
  rekey 14400
cipher-suite aes256-cbc-shal
group 14
  authentication-type
  pre-shared-key-dynamic
  
  !
ipsec
  rekey 3600
  replay-window 512
cipher-suite null-shal
  perfect-forward-secrecy group-16
  
  !
  mtu 1400
  no shutdown
  !
interface ipsec2
  ip unnumbered
tunnel-source-interface ge0/0
tunnel-destination dynamic
tunnel-set secure-internet-gateway-umbrella
tunnel-dc-preference secondary-dc
ike
    version 2
    rekey 14400
    cipher-suite aes256-cbc-shal
    group 14
    authentication-type
      pre-shared-key-dynamic
    !

! ipsec
    rekey 3600
    replay-window 512
    cipher-suite null-shal
    perfect-forward-secrecy group-16
    !
    mtu 1400
    no shutdown
    !
    ip route 0.0.0.0/0 10.0.0.254
    !

vpn 1
  dns-redirect umbrella
  interface ge0/2
    ip address 10.0.0.253/24
    no shutdown
    !
  ip service-route 0.0.0.0/0 vpn 0 service sig
  !
vpn 512
  name vpn512
  interface eth0
    ip address 10.30.1.64/24
    no shutdown
  !

Appendix C: Configuring Tenant Controls

This test case involves creating the tenant controls for Google G Suite to prevent users accessing accounts outside of the company domain.

Procedure 1. Create the Tenant Control

  Step 1. In Umbrella, navigate to Policies > Policy Components > Tenant Controls.
Step 2. In the top right corner, click Add.

Step 3. Add a meaningful name to the policy and choose the cloud app or suite you wish to approve. This test will cover Google G Suite. Click Google G Suite.

Step 4. Enter the domain(s) that you wish to provide access to and click Add. Save the policy.
Procedure 2. Add Tenant Control to Web Policy

Step 1. In Umbrella, navigate to Policies > Management > Web Policies.

Step 2. Click the policy you wish to edit. For this test, the policy protecting the branch network will be used.

Step 3. Click Edit under Tenant Controls.
<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Protection Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDWAN</td>
<td>2 Identities Affected</td>
</tr>
<tr>
<td></td>
<td>- 2 Tunnels</td>
</tr>
<tr>
<td></td>
<td>- Edit Identity</td>
</tr>
<tr>
<td></td>
<td>Security Setting Applied: Default Web Settings</td>
</tr>
<tr>
<td></td>
<td>Command and Control Callbacks, Malware, and Phishing Attacks will be blocked</td>
</tr>
<tr>
<td></td>
<td>No integration is enabled.</td>
</tr>
<tr>
<td></td>
<td>- Edit Disable</td>
</tr>
<tr>
<td></td>
<td>Content Setting Applied: Default Web Settings</td>
</tr>
<tr>
<td></td>
<td>No categories will be blocked.</td>
</tr>
<tr>
<td></td>
<td>- Edit Disable</td>
</tr>
<tr>
<td></td>
<td>Tenant Controls Applied: CVD Tenant Controls</td>
</tr>
<tr>
<td></td>
<td>branchsite.net and Slack Workspace 445d9970-1598043392-583</td>
</tr>
<tr>
<td></td>
<td>- Edit Disable</td>
</tr>
<tr>
<td></td>
<td>0 Destination List Enforced</td>
</tr>
<tr>
<td></td>
<td>- Enable</td>
</tr>
<tr>
<td></td>
<td>File Analysis Enabled</td>
</tr>
<tr>
<td></td>
<td>- File Inspection Enabled</td>
</tr>
<tr>
<td></td>
<td>- Threat Grid Malware Analysis Not Enabled</td>
</tr>
<tr>
<td></td>
<td>- Edit</td>
</tr>
<tr>
<td></td>
<td>File Type Control Enabled</td>
</tr>
<tr>
<td></td>
<td>- exe will be blocked</td>
</tr>
<tr>
<td></td>
<td>- Edit Disable</td>
</tr>
<tr>
<td></td>
<td>Umbrella Default Block Page Applied</td>
</tr>
<tr>
<td></td>
<td>- Edit</td>
</tr>
<tr>
<td></td>
<td>HTTPS Inspection Enabled</td>
</tr>
<tr>
<td></td>
<td>- No categories or domains exempted</td>
</tr>
<tr>
<td></td>
<td>- Edit</td>
</tr>
</tbody>
</table>
Step 4. Using the dropdown list, select the tenant control policy created in the previous step. Click **Set & return**.

Procedure 3. Testing the policy

**Step 1.** On a client device that will be assigned to the identity created in the policy above, navigate to gmail.com. For the purposes of this test, a Ubuntu device was used, connected to SIG via the vedge router in the branch network. If the policy was applied correctly, a block page will be shown like below.

Appendix D: Configuring File Policies

This test case involves creating file policy to block users from downloading files with a .exe extension. This will block all executable files regardless if it is harmful to the device.

**Procedure 1. Apply File type control to Web Policy**

**Step 1.** In Umbrella, navigate to Policies > Management > Web Policies.
Step 2. Click the policy you wish to edit. For this test, the policy protecting the branch network will be used.

Step 3. Click Edit under File type control.

Step 4. Choose the files you would like to be blocked. For this test exe files were chosen and will be disabled from passing through SIG. Click Set & return. Click save.
Procedure 2. Testing the policy

Step 1. On a client device that will be assigned to the identity created in the policy above, attempt to download a file type that has been blocked in the policy. For the purposes of this test, a Ubuntu device was used, connected to SIG via the vedge router in the branch network and we attempted to download a .exe file. In Umbrella, navigate to Reporting > Core Reports > Activity Search to ensure the policy was applied correctly and that the correct policy has been matched.