

Best Practices für Cisco Umbrella-Benutzer

Inhalt

[Einleitung](#)

[Cisco Umbrella Service - Status und Systemstatus](#)

[Netzwerkregistrierung](#)

[Lokale Firewalls und Proxys](#)

[Die Einführungsphase](#)

[Seite "Intelligent Proxy/Block"](#)

[Virtuelle Cisco Umbrella-Appliances](#)

[Integration mit Drittanbieterlösungen](#)

[Active Directory-Integration](#)

[Roaming-Clients](#)

[Protokollieren](#)

[Best Practices für die Managed Services-Konsole](#)

[Zwei-Faktor-Authentifizierung](#)

[Kontaktaufnahme und Zusammenarbeit mit dem Cisco Umbrella Support Team](#)

Einleitung

In diesem Dokument werden verschiedene Best Practices im Zusammenhang mit Cisco Umbrella beschrieben.

Cisco Umbrella Service - Status und Systemstatus

- Setzen Sie ein Lesezeichen <http://208.69.38.170/> und <https://146.112.59.2/#/>, damit Sie die Seiten für den Umbrella-Systemstatus überprüfen können, auch wenn der lokale DNS nicht verfügbar ist.
- Abonnieren Sie die Cisco Umbrella Service Status-Seite unter <https://146.112.59.2/#/>, um Benachrichtigungen über Service-Beeinträchtigungen, Service-Ausfälle und/oder Wartung und Ereignisse zu erhalten.
- Folgen Sie den Seiten für Service-Updates und -Ankündigungen in der Cisco Umbrella Knowledge Base.
- Überprüfen Sie regelmäßig das Cisco Umbrella Dashboard "Message Center" auf Produktwarnungen und Benachrichtigungen.

Netzwerkregistrierung

Alle Ihrer Organisation zugeordneten IP-Adressen und IP-Adressen-CIDR-Bereiche müssen bei Umbrella registriert sein. Weitere Informationen finden Sie in [der Umbrella-Dokumentation](#).

Lokale Firewalls und Proxys

- Konfigurieren Sie lokale Firewalls, um Umbrella IP address CIDR-Bereiche zuzulassen.
- Wenn Sie einen HTTP-Proxy verwenden, stellen Sie sicher, dass dieser konfiguriert ist.

Die Einführungsphase

- Führen Sie die Bereitstellung möglichst schrittweise durch, und testen Sie sie vor der Bereitstellung in großen Mengen. Um neue Funktionen zu testen, wenden Sie eine Richtlinie auf eine Untergruppe von Benutzern und Computern an. Wenn der Test erfolgreich war, wenden Sie die Richtlinie auf mehr Benutzer und Computer an.
- Verwenden Sie den Richtlinien tester, um die beabsichtigte Richtlinienfunktionalität für Identitäten und einzelne Domänen zu überprüfen.
- Überprüfen Sie die Funktionalität, indem Sie die Testseiten mit einem Browser aufrufen. Weitere Informationen finden Sie unter: Vorgehensweise: Führen Sie einen erfolgreichen Test durch, um sicherzustellen, dass Sie Umbrella ordnungsgemäß ausführen.
- Erstellen Sie einen oder mehrere Zeitgesteuerte Berichte, um Ihre Umgebung auf sicherheitsrelevante Ereignisse zu überwachen. Weitere Informationen hierzu finden Sie in der [Umbrella-Dokumentation](#).

Seite "Intelligent Proxy/Block"

- Integrieren Sie die [Stammzertifizierungsstelle](#) in Ihre Einführung, insbesondere wenn Sie die Intelligent Proxy-Funktionen verwenden oder dies planen. Es ist auch eine gute Idee, es trotzdem zu installieren, da Websites blockiert werden, wenn sie https:// sind (zB: <https://facebook.com>) Fehler erzeugen, ohne dass dies der Fall ist.

Virtuelle Cisco Umbrella-Appliances

- Wenn Sie virtuelle Appliances (VAs) verwenden, stellen Sie sicher, dass die Liste [Interne Domänen](#) vor der Bereitstellung ausgefüllt wird.
- Wenn Sie virtuelle Appliances auf VMWare verwenden, verwenden Sie entsprechend VMXNET3-Adapter.
- Wenn Sie virtuelle Appliances verwenden, überprüfen Sie in regelmäßigen Abständen die Konsole der VA über den VMWare- oder Hyper-V-Host. Auf der rechten Seite werden alle Einträge für Services und Konnektivität als grün angezeigt.
- Konfigurieren Sie die internen DNS-Server wie folgt: Welche Konfiguration wird für interne DNS-Server bei der Bereitstellung von Umbrella empfohlen?

Integration mit Drittanbieterlösungen

- Wenn Sie Integrationen wie Check Point oder Cisco AMP Threat Grid verwenden, fügen Sie der globalen Zulassungsliste (oder anderen Domänenlisten gemäß Ihren Umbrella-Richtlinien) Domänen hinzu, die nie gesperrt werden sollen:

- Die Startseite für Ihr Unternehmen (mydomain.com).
- Domänen, die von Ihnen bereitgestellte Services repräsentieren und sowohl interne als auch externe Datensätze enthalten können (mail.myservicedomain.com, portal.myotherservicedomain.com).
- Es kann weniger bekannte Cloud-Anwendungen geben, von denen Sie in hohem Maße abhängig sind, da Cisco Umbrella die automatische Domänenvalidierung kennt oder nicht berücksichtigt (localcloudservice.com)

Active Directory-Integration

- Wenn Cisco Umbrella in Active Directory integriert ist, fügen Sie der [Liste AD-Benutzerausnahmen](#) Dienstkonto hinzu.

Roaming-Clients

- Wenn Sie Roaming-Clients verwenden, stellen Sie sicher, dass die [Liste Interne Domänen](#) ausgefüllt ist.
- Vergewissern Sie sich, dass alle Ihre Roaming-Clients im Cisco Umbrella Dashboard unter Identitäten > Roaming-Computer auf derselben Version installiert sind.
- Bei Verwendung des Cisco Secure Client (ehemals AnyConnect) sollte das Umbrella Roaming Security Module anstelle des Standalone Roaming Client verwendet werden.
- Wenn Sie einen Roaming-Client in einem Wi-Fi-Netzwerk einer Fluggesellschaft verwenden, finden Sie weitere Informationen unter Roaming-Client und Wi-Fi-Best Practices für Fluggesellschaften/Hotels.

Protokollieren

Die detaillierten Protokolle werden nur 30 Tage lang aufbewahrt und dann in aggregierte Berichtsdaten aufgegliedert. Wenn Sie eine Kopie der detaillierteren Daten länger als 30 Tage aufbewahren möchten, richten Sie einen Amazon S3-Bucket ein, in den Sie Ihre Daten exportieren können, unter Einstellungen > Protokollverwaltung.

Best Practices für die Managed Services-Konsole

Managed Services Console MSP Professional Services Automation (PSA)-Integration:

- Wenn Sie ein [MSP](#) sind, der [in einen PSA integriert ist](#), stellen Sie sicher, dass das Symbol "PSA INTEGRATION" grün angezeigt wird.

Zwei-Faktor-Authentifizierung

- [Zwei-Faktor-Authentifizierung](#) für Cisco Umbrella-Benutzer implementieren
- Implementieren Sie die Zwei-Schritt-Authentifizierung für Cisco Umbrella MSP-Administratoren.

Kontaktaufnahme und Zusammenarbeit mit dem Cisco Umbrella Support Team

- Senden Sie nach der Anmeldung beim Umbrella Dashboard über das Webformular auf der Anforderungsseite eine Anfrage an das Umbrella Support Team.
- Wenn Sie Telefonsupport von Cisco Umbrella erworben haben, wird oben rechts im Cisco Umbrella Dashboard ein Telefonsymbol angezeigt. Klicken Sie auf das Telefonsymbol, um die Telefonnummer für den Support anzuzeigen.
- Geben Sie vollständige Details zu Ihren Problemen oder Fragen an.
- Verwenden Sie die Ausgabe des Umbrella Diagnostic Tools für Ihren Support-Fall.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.