Blockieren unbekannter Anwendungen auf einer sicheren Webappliance

Inhalt

[Einleitung](#)
[Methoden zum Blockieren unbekannter Anwendungen](#)
[Blockieren von Anwendungen basierend auf Benutzer-Agent-Strings](#)
[Blockieren von Anwendungen auf Basis von Anwendungstransparenzkontrollen](#)
[Blockieren von Anwendungen basierend auf MIME-Typ](#)
[URL-Kategorien in Zugriffsrichtlinien sperren](#)
[Einschränkung der Konfiguration von HTTP CONNECT-Ports in der Zugriffsrichtlinie](#)
[Zugriff für bestimmte IP-Adressen sperren](#)
[Ermitteln, welcher Benutzer-Agent oder MIME-Typ von einer Anwendung verwendet wird](#)
[Referenz](#)
[Liste der Benutzer-Agents](#)
[Liste der MIME-Typen](#)

Einleitung

In diesem Dokument werden verschiedene Methoden zum Blockieren unbekannter Anwendungen auf der Cisco Secure Web Appliance beschrieben.

Methoden zum Blockieren unbekannter Anwendungen

Sie können eine dieser Methoden allein oder in Kombination verwenden.

> **Anmerkung:** Dieser Knowledge Base-Artikel bezieht sich auf Software, die nicht von Cisco verwaltet oder unterstützt wird. Die Informationen werden Ihnen zu Ihrer Zufriedenheit zur Verfügung gestellt. Wenden Sie sich für weitere Unterstützung an den Softwareanbieter.

Blockieren von Anwendungen basierend auf Benutzer-Agent-Strings

Die erste Verteidigung besteht darin, Benutzer-Agent-Zeichenfolgen zu verwenden, um unbekannte Anwendungen zu blockieren.

- Fügen Sie den Benutzer-Agent unter **Web Security Manager** > **Access Policies** > **Protocols and User Agents** Spalte <für die erforderliche Zugriffsrichtlinie>.
- Fügen Sie die User Agent-Zeichenfolge unter **Block Custom User Agents** (eine pro Leitung).

> **Anmerkung:** Sie können die unter Referenz bereitgestellten Links verwenden, um nach Benutzer-Agents zu suchen.

Blockieren von Anwendungen auf Basis von Anwendungstransparenzkontrollen

Wenn Application Visibility Controls (AVC) aktiviert sind (unter **GUI > Security Services > Web Reputation and Anti-Malware**), dann können Sie den Zugriff auf Basis von Anwendungstypen wie Proxys, Dateifreigabe, Internetdienstprogramme usw. blockieren. Sie können dies unter **Web Security Manager > Access Policies > Applications** Spalte <für die erforderliche Zugriffsrichtlinie>.

Blockieren von Anwendungen basierend auf MIME-Typ

Wenn der Benutzer-Agent nicht vorhanden ist, können Sie versuchen, den MIME-Typ (Multipurpose Internet Mail Extensions) hinzuzufügen:

- MIME-Typen unter **Web Security Manager** > **Web Access Policies** > **Objects** Spalte <für die erforderliche Zugriffsrichtlinie>.
- Fügen Sie das Objekt/den MIME-Typ in das Feld **Block Custom MIME Types** -Abschnitt (eine pro Zeile). Um beispielsweise BitTorrent-Anwendungen zu blockieren, geben Sie application/x-bittorrent.

  Anmerkung: Sie können die unter Referenz bereitgestellten Links verwenden, um nach MIME-Typen zu suchen.

URL-Kategorien in Zugriffsrichtlinien sperren

Stellen Sie sicher, dass Kategorien wie Filtervermeidung, illegale Aktivitäten, illegale Downloads usw. in Zugriffsrichtlinien blockiert werden. Wenn einige Anwendungen bekannte URLs oder IP-Adressen für ihre Verbindungen verwenden, können Sie die zugehörigen vordefinierten URL-Kategorien blockieren oder sie in einer blockierten benutzerdefinierten URL-Kategorie konfigurieren, indem Sie ihre IP-Adresse, Fully Qualified Domain Name (FQDN) oder einen regulären Ausdruck verwenden, der den Domänen entspricht. Sie können dies unter **Web Security Manager > Access Policies > URL Categories** Spalte.

Einschränkung der Konfiguration von HTTP CONNECT-Ports in der Zugriffsrichtlinie

Einige Anwendungen können die HTTP CONNECT-Methode verwenden, um eine Verbindung zu verschiedenen Ports herzustellen. Lassen Sie nur bekannte Ports oder die spezifischen Ports zu, die in Ihrer Umgebung in den Konfigurationsdomänen für HTTP CONNECT-Ports benötigt werden:

- HTTP CONNECT kann unter **Web Security Manager** > **Access Policies** > **Protocols and User Agents** Spalte <für die erforderliche Zugriffsrichtlinie>.
- Zulässige Ports hinzufügen unter **HTTP CONNECT Ports**.

Zugriff für bestimmte IP-Adressen sperren

Bei Anwendungen, bei denen Sie nur über Ziel-IP-Adressen Bescheid wissen, auf die zugegriffen wird, können Sie mithilfe der L4-Datenverkehrsüberwachungsfunktion den Zugriff für diese spezifischen IP-Adressen blockieren. Sie können die Ziel-IPs unter **Web Security Manager > L4 Traffic Monitor > Additional Suspected Malware Addresses**.

Ermitteln, welcher Benutzer-Agent oder MIME-Typ von einer Anwendung verwendet wird

Wenn Sie nicht wissen, welcher Benutzer-Agent oder MIME-Typ von bestimmten Anwendungen verwendet wird, können Sie einen der folgenden Schritte ausführen, um diese Informationen zu finden:

- Führen Sie eine Paketerfassung mit WireShark (Ethereal) auf dem Computer des Clients aus, und filtern Sie nach dem Protokoll 'http'.
- Führen Sie die Erfassung auf der sicheren Web-Appliance aus (unter **Support and Help** > **Packet Capture**), gefiltert auf die IP-Adresse des Clients.

Referenz

> **Anmerkung:** Die hier aufgeführten externen Websites dienen lediglich als Referenz. Links und Inhalte werden nicht von Cisco kontrolliert und können geändert werden.

Liste der Benutzer-Agents

User Agent String.Com (unter useragentString.com)

Liste der MIME-Typen

- Gängige MIME-Typen (bei mozilla.org)
- MIME-Typen: Vollständige Liste der MIME-Typen (auf w3cub.com)
- Vollständige Liste der MIME-Typen (unter sitepoint.com)