Come bloccare applicazioni sconosciute su Secure Web Appliance

Sommario

Introduzione

In questo documento vengono descritti diversi metodi per bloccare applicazioni sconosciute su Cisco Secure Web Appliance.

Metodi per bloccare applicazioni sconosciute

Èpossibile utilizzare uno di questi metodi singolarmente o in combinazione.

> **Nota:** Questo articolo della Knowledge Base fa riferimento a software non gestito o supportato da Cisco. Le informazioni sono fornite a titolo di cortesia. Per ulteriore assistenza, contattare il fornitore del software.

Blocca applicazioni basate su stringhe agente utente

La prima difesa consiste nell'utilizzare le stringhe dell'agente utente per bloccare le applicazioni sconosciute.

- Aggiungi agente utente in **Web Security Manager** > **Access Policies** > **Protocols and User Agents** colonna <per il criterio di accesso richiesto>.
- Aggiungere la stringa Agente utente in **Block Custom User Agents** (uno per riga).

> **Nota:** È possibile utilizzare i collegamenti forniti in Riferimento per cercare gli agenti utente.

Blocca applicazioni in base ai controlli di visibilità delle applicazioni

Se i controlli di visibilità delle applicazioni (AVC) sono attivati (in **GUI > Security Services > Web Reputation and Anti-Malware**), quindi è possibile bloccare l'accesso in base a tipi di applicazioni quali proxy, condivisione file, utilità Internet e così via. È possibile eseguire questa operazione in **Web Security Manager > Access Policies > Applications** colonna <per il criterio di accesso richiesto>.

Blocca applicazioni basate sul tipo MIME

Se l'agente utente non esiste, è possibile tentare di aggiungere il tipo MIME (Multipurpose Internet Mail Extensions):

- Aggiungi tipi MIME in **Web Security Manager** > **Web Access Policies** > **Objects** colonna <per il criterio di accesso richiesto>.
- Aggiungere il tipo object/MIME nel **Block Custom MIME Types** (una per riga). Ad esempio, per bloccare le applicazioni BitTorrent, immettere: application/x-bittorrent.

Nota: È possibile utilizzare i collegamenti forniti in Riferimento per cercare i tipi MIME.

Blocca categorie URL nei criteri di accesso

Verificare che nei criteri di accesso categorie quali Prevenzione filtro, Attività illecite, Download illeciti e così via siano bloccate. Se alcune applicazioni utilizzano URL o indirizzi IP noti per le connessioni, è possibile bloccare le categorie URL predefinite associate o configurarle in una categoria URL personalizzata bloccata utilizzando l'indirizzo IP, il nome di dominio completo (FQDN) o un regex corrispondente ai domini. È possibile eseguire questa operazione in **Web Security Manager > Access Policies > URL Categories** colonna.

Limita la configurazione delle porte di connessione HTTP nei criteri di accesso

Alcune applicazioni possono utilizzare il metodo CONNECT HTTP per connettersi a porte diverse. Consenti solo porte conosciute o porte specifiche necessarie nell'ambiente nei domini di configurazione delle porte HTTP CONNECT:

- HTTP CONNECT può essere configurato in **Web Security Manager** > **Access Policies** > **Protocols and User Agents** colonna <per il criterio di accesso richiesto>.
- Aggiungi porte consentite in **HTTP CONNECT Ports**.

Accesso a blocchi per indirizzi IP specifici

Per le applicazioni in cui si conoscono solo gli indirizzi IP di destinazione a cui si accede, è possibile utilizzare la funzionalità L4 Traffic Monitor per bloccare l'accesso a tali indirizzi IP specifici. È possibile aggiungere gli IP di destinazione in **Web Security Manager > L4 Traffic Monitor > Additional Suspected Malware Addresses**.

Come individuare l'agente utente o il tipo MIME utilizzato da un'applicazione

Se non si conosce l'agente utente o il tipo MIME utilizzato da alcune applicazioni, è possibile eseguire una delle seguenti operazioni per trovare le informazioni:

- Eseguire un'acquisizione pacchetto con WireShark (Ethernet) sul computer del client e filtrare per il protocollo 'http'.
- Eseguire l'acquisizione su Secure Web Appliance (in **Support and Help** > **Packet Capture**), filtrati in base all'indirizzo IP del client.

Riferimento

> **Nota:** I siti Web esterni elencati sono forniti solo a scopo di riferimento. I link e i contenuti non sono controllati da Cisco e sono soggetti a modifiche.

Elenco di agenti utente

String.Com agente utente (all'indirizzo useragentstring.com)

Elenco di tipi MIME

- Tipi MIME comuni (all'indirizzo mozilla.org)
- Tipi MIME: Elenco completo dei tipi MIME (all'indirizzo w3cub.com)
- Elenco completo dei tipi MIME (all'indirizzo sitepoint.com)