In che modo Cisco Web Security Appliance (WSA) gestisce il traffico Skype?

Sommario

Domanda:

In che modo Cisco Web Security Appliance (WSA) gestisce il traffico Skype?

Ambiente: Cisco WSA, Skype

Skype è una rete di telefonia Internet (VoIP) proprietaria. Skype opera principalmente come programma peer-to-peer, quindi non comunica direttamente con un server centrale per funzionare. Skype può essere particolarmente difficile da bloccare, in quanto tenterà di connettersi in molti modi diversi.

Skype si connette nel seguente ordine di preferenza:

1. Indirizzare pacchetti UDP ad altri peer utilizzando numeri di porta casuali
2. Indirizza i pacchetti TCP ad altri peer utilizzando numeri di porta casuali
3. Indirizzare i pacchetti TCP ad altri peer utilizzando la porta 80 e/o la porta 443
4. Pacchetti tunneling tramite proxy Web con HTTP CONNECT alla porta 443

Se implementati in un ambiente proxy esplicito, i metodi da 1 a 3 non verranno mai inviati al Cisco WSA. Per bloccare Skype, deve prima essere bloccato da un altro punto della rete. Le fasi 1-3 di Skype possono essere bloccate usando:

- Firewall Usa NBAR per bloccare Skype versione 1. Ulteriori informazioni sono disponibili all'indirizzo http://ciscotips.wordpress.com/2006/06/07/how-to-block-skype/
- Cisco IPS (ASA): Cisco ASA può potenzialmente rilevare e bloccare Skype tramite firme.

Quando Skype torna a utilizzare un proxy esplicito, Skype non fornisce deliberatamente alcun dettaglio del client nella richiesta HTTP CONNECT (nessuna stringa agente utente). Ciò rende difficile distinguere tra Skype e una richiesta CONNECT valida. Skype si collegherà sempre alla porta 443 e l'indirizzo di destinazione è sempre un indirizzo IP.

Esempio:

CONNECT 10.129.88.111:443 HTTP/1.0
Connessione proxy: keep-alive

I seguenti criteri di accesso bloccheranno qualsiasi richiesta CONNECT tramite il WSA che corrisponda agli indirizzi IP e alla porta 443. Questo criterio corrisponderà a tutto il traffico Skype. Tuttavia, anche i programmi non Skype che tentano di eseguire il tunnel a un indirizzo IP sulla

porta 443 verranno bloccati.

Blocco di Skype - Ambiente esplicito con il proxy HTTPS disabilitato

Creare una categoria URL personalizzata che corrisponda al traffico IP e alla porta 443:

1. Selezionare "Security Manager" -> "Custom URL Categories" -> "Add Custom Category" (Aggiungi categoria personalizzata).
2. Compilare "Category Name" ed espandere "Advanced".
3. Utilizzare "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+" nella finestra Espressione regolare.

Impostare questa categoria su Nega nei criteri di accesso:

1. Passare a "Web Security Manager" -> "Access Policies" (Policy di accesso).
2. Fare clic sul collegamento nella colonna "Categorie URL" per il gruppo di criteri appropriato.
3. Nella sezione "Custom URL Category Filtering", scegli "Block" (Blocca) per la nuova categoria Skype.
4. Invia e conferma le modifiche

Nota: Le richieste CONNECT esplicite possono essere bloccate solo se il servizio proxy HTTPS è disabilitato.

Quando la decrittografia HTTPS di WSA è abilitata, il traffico Skype potrebbe molto probabilmente interrompersi perché non si tratta solo di traffico HTTPS (nonostante si utilizzi CONNECT e la porta 443). Verrà generato un errore 502 da WSA e la connessione verrà interrotta. Qualsiasi traffico Web HTTPS reale verso un indirizzo IP continuerà a funzionare (anche se verrà decriptato sul WSA).

Blocco di Skype - Ambiente esplicito/trasparente con il proxy HTTPS abilitato

Creare una categoria personalizzata che corrisponda al traffico IP e alla porta 443:

1. Selezionare "Security Manager" -> "Custom URL Categories" -> "Add Custom Category" (Aggiungi categoria personalizzata).
2. Compilare "Category Name" ed espandere "Advanced".
3. Utilizzare "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+" nella finestra Espressione regolare.

Impostare questa categoria per la decrittografia nei criteri di decrittografia:

1. Selezionare "Web Security Manager" -> "Decryption Policies" (Criteri di decrittografia).
2. Fare clic sul collegamento nella colonna "Categorie URL" per il gruppo di criteri appropriato.
3. Nella sezione "Custom URL Category Filtering", scegli "Decrypt" (Decrittografa) per la nuova categoria Skype.
4. Inviare e confermare le modifiche.

Nota: Poiché il traffico Skype viene inviato a un IP, verrà considerato come parte degli "URL non classificati". Lo stesso effetto si verificherà a seconda che l'azione sia decrittografata o passthrough.