Abilitare il preprocessore di normalizzazione in linea e comprendere l'ispezione pre-ACK e post-ACK

Sommario

Introduzione

In questo documento viene descritto come attivare il preprocessore di normalizzazione in linea e viene illustrato come identificare la differenza e l'impatto di due opzioni avanzate di normalizzazione in linea.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza del sistema Cisco Firepower e di Snort.

Componenti usati

Le informazioni fornite in questo documento si basano sui dispositivi Cisco FireSIGHT Management Center e Firepower.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Un preprocessore di normalizzazione in linea normalizza il traffico in modo da ridurre al minimo la possibilità che un utente non autorizzato possa eludere il rilevamento utilizzando le distribuzioni in linea. La normalizzazione avviene immediatamente dopo la decodifica del pacchetto e prima di qualsiasi altro preprocessore, e procede dagli strati interni del pacchetto verso l'esterno. La normalizzazione in linea non genera eventi, ma prepara i pacchetti per l'utilizzo da parte di altri preprocessori.

Quando si applica un criterio di intrusione con il preprocessore di normalizzazione in linea attivato, il dispositivo Firepower verifica queste due condizioni per garantire che venga utilizzata una distribuzione in linea:

- Nelle versioni 5.4 e successive, la *modalità in linea* è attivata nei criteri di analisi della rete e anche l'opzione *Elimina quando in linea* è configurata nei criteri antintrusione se questi ultimi sono impostati per eliminare il traffico. Per le versioni 5.3 e precedenti, l'opzione *Elimina quando inline* è abilitata nei criteri per le intrusioni.

- Il criterio viene applicato a un set di interfacce inline (o inline con failopen).

Pertanto, oltre all'attivazione e alla configurazione del preprocessore di normalizzazione in linea, è necessario verificare che questi requisiti siano soddisfatti, altrimenti il preprocessore non normalizzerà il traffico:

- Ènecessario impostare i criteri in modo da eliminare il traffico nelle distribuzioni inline.

- Ènecessario applicare il criterio a un set in linea.

Abilita normalizzazione in linea

In questa sezione viene descritto come abilitare la normalizzazione in linea per le versioni 5.4 e successive e per le versioni 5.3 e precedenti.

Abilita normalizzazione in linea nelle versioni 5.4 e successive

La maggior parte delle impostazioni del preprocessore è configurata in Protezione accesso alla rete per le versioni 5.4 e successive. Completare questi passaggi per abilitare la normalizzazione in linea in Protezione accesso alla rete:

1. Accedere all'interfaccia utente Web del centro di gestione FireSIGHT.

2. Passare a **Policy > Controllo accesso**.

3. Fare clic su **Criteri di analisi della rete** nella parte superiore destra della pagina.

4. Selezionare un *criterio di analisi della rete* da applicare al dispositivo gestito.

5. Fare clic sull'icona a forma di *matita* per iniziare la modifica. Verrà visualizzata la pagina *Modifica criterio*.

6. Fare clic su **Settings** (Impostazioni) sul lato sinistro della schermata per visualizzare la pagina *Settings* (Impostazioni).

7. Individuare l'opzione **Normalizzazione in linea** nell'area *Preprocessore livello di rete/trasporto*.

8. Per abilitare questa funzione, selezionare il pulsante di opzione **Enabled**:

Affinché venga eseguita la normalizzazione in linea, è necessario aggiungere Protezione accesso alla rete con la normalizzazione in linea ai criteri di controllo di accesso. È possibile aggiungere Protezione accesso alla rete tramite la scheda *Avanzate* dei criteri di controllo di accesso:

I criteri di controllo di accesso devono quindi essere applicati al dispositivo di controllo.

> **Nota:** Per la versione 5.4 o successive, è possibile abilitare la normalizzazione in linea per determinati traffici e disabilitarla per altri. Se si desidera abilitarla per il traffico specifico, aggiungere una *regola di analisi della rete* e impostare i criteri e i criteri del traffico su quello per cui è abilitata la normalizzazione in linea. Se si desidera attivarlo globalmente, impostare il *criterio di analisi di rete predefinito* su quello per cui è attivata la normalizzazione in linea.

Abilita normalizzazione in linea nelle versioni 5.3 e precedenti

Completare questi passaggi per abilitare la normalizzazione in linea in un criterio per le intrusioni:

1. Accedere all'interfaccia utente Web del centro di gestione FireSIGHT.

2. Selezionare **Criteri > Intrusione > Criteri intrusione**.

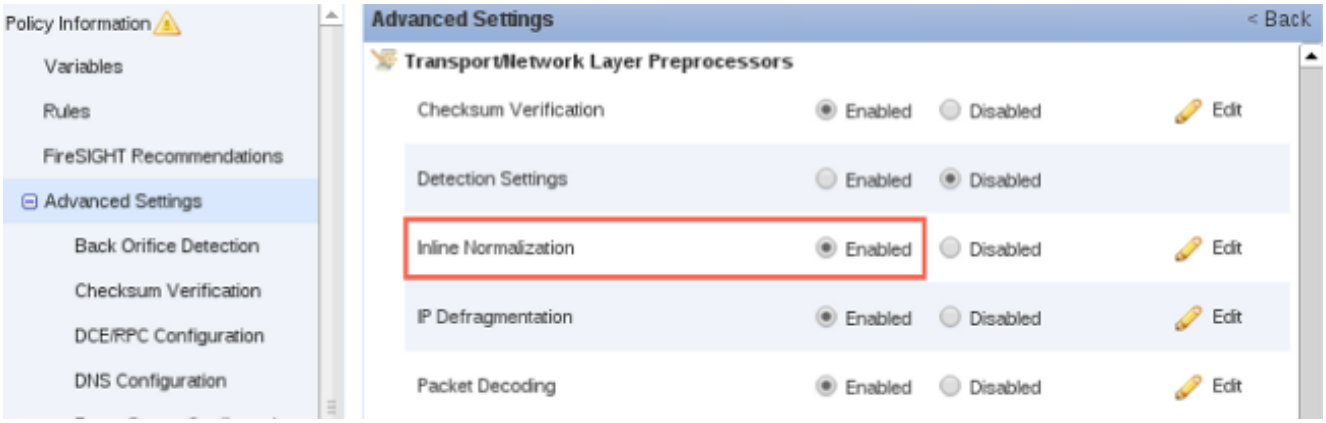
3. Selezionare un *criterio di intrusione* da applicare al dispositivo gestito.

4. Fare clic sull'icona a forma di *matita* per iniziare la modifica. Verrà visualizzata la pagina *Modifica criterio*.

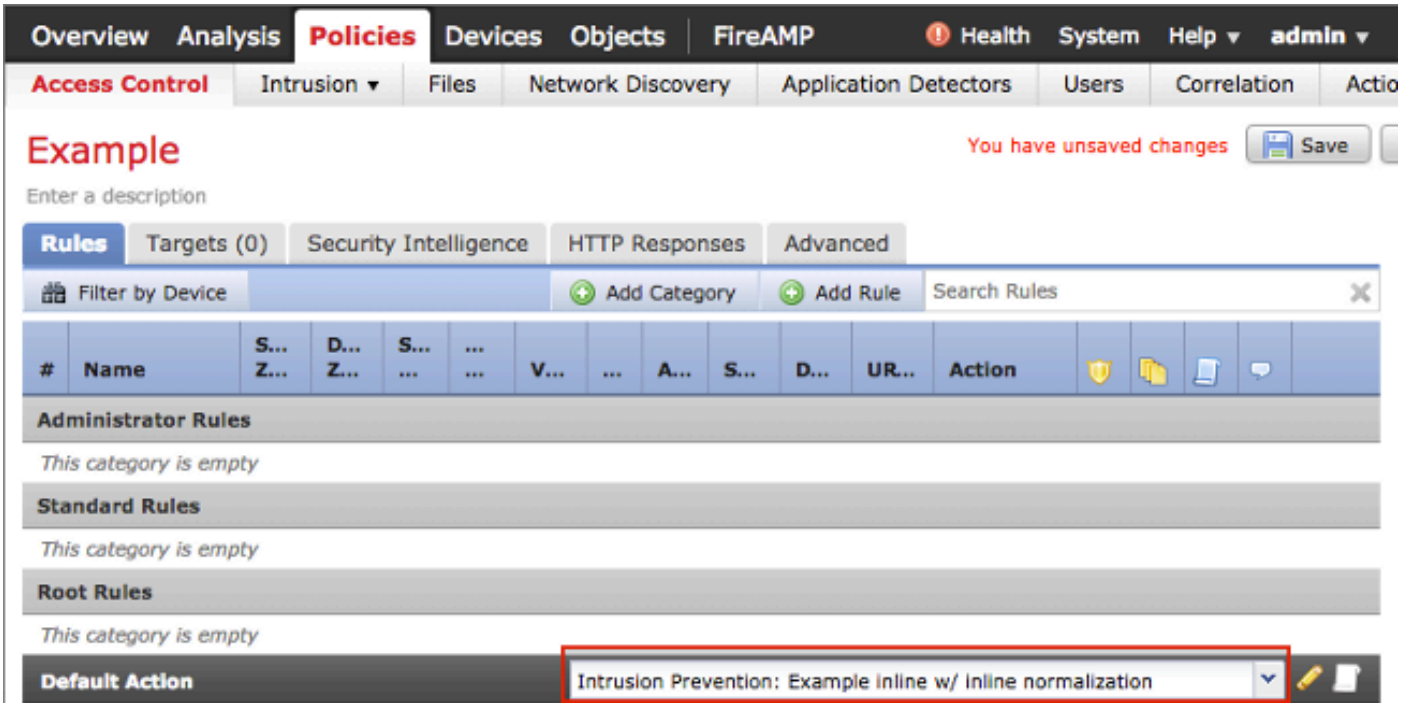
5. Fare clic su **Impostazioni avanzate** per visualizzare la pagina *Impostazioni avanzate*.

6. Individuare l'opzione **Normalizzazione in linea** nell'area *Preprocessore livello di rete/trasporto*.

7. Per abilitare questa funzione, selezionare il pulsante di opzione **Enabled**:



Dopo aver configurato il criterio di intrusione per la normalizzazione in linea, è necessario aggiungerlo come azione predefinita nel criterio di controllo di accesso:



I criteri di controllo di accesso devono quindi essere applicati al dispositivo di controllo.

Èpossibile configurare il preprocessore di normalizzazione in linea per normalizzare il traffico IPv4, IPv6, ICMPv4 (Internet Control Message Protocol Version 4), ICMPv6 e TCP in qualsiasi combinazione. La normalizzazione di ogni protocollo viene eseguita automaticamente quando la normalizzazione del protocollo è attivata.

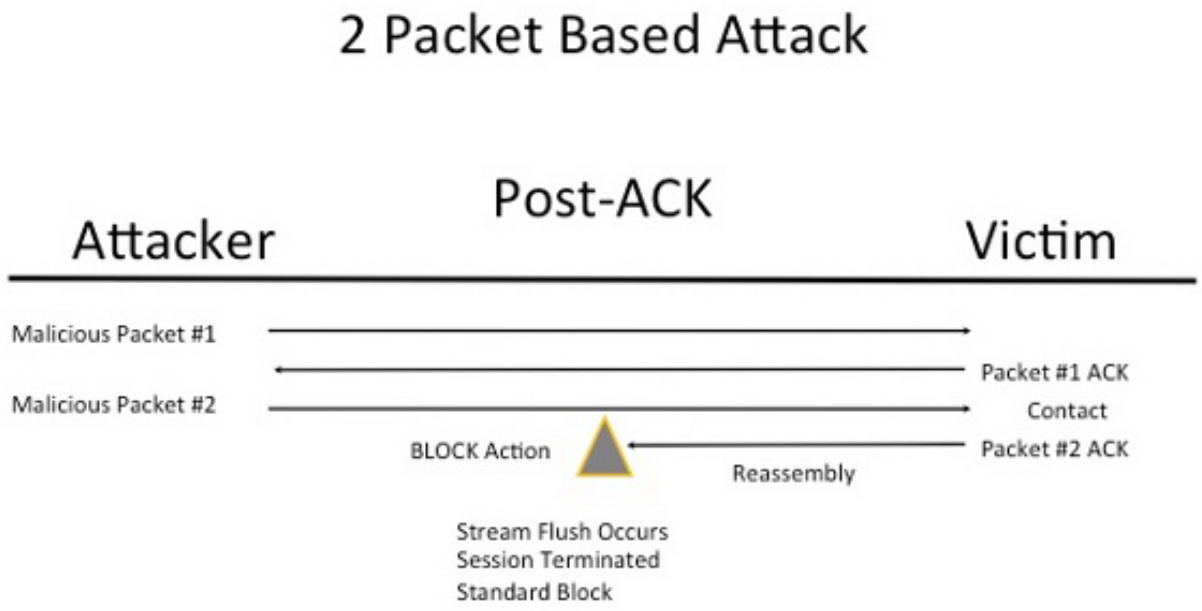
Abilita ispezione post-ACK e ispezione pre-ACK

Dopo aver abilitato il preprocessore di normalizzazione in linea, è possibile modificare le impostazioni per abilitare l'opzione *Normalize TCP Payload*. Questa opzione del preprocessore di normalizzazione in linea passa da una modalità di ispezione all'altra:

- Post-riconoscimento (Post-ACK)
- Pre-riconoscimento (Pre-ACK)

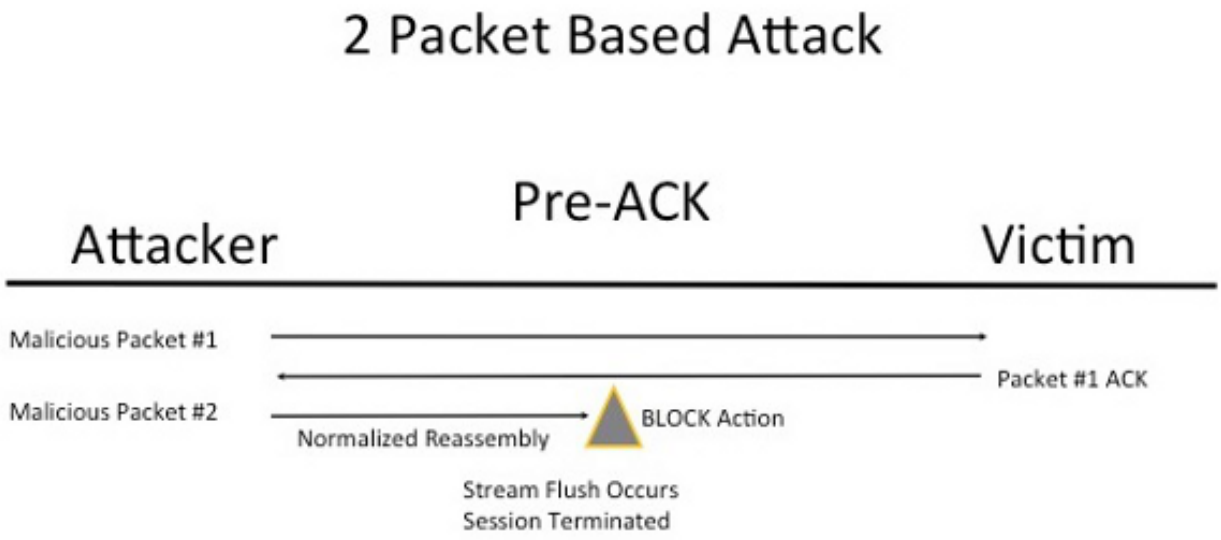
Informazioni sull'ispezione post-ACK (normalizzazione del payload TCP/normalizzazione disabilitata)

Nell'ispezione post-ACK, il riassemblaggio del flusso di pacchetti, lo svuotamento (consegna al resto del processo di ispezione) e il rilevamento in Snort si verificano dopo che la conferma (ACK) da parte della vittima per il pacchetto che completa l'attacco è stata ricevuta dal sistema di prevenzione delle intrusioni (IPS). Prima che si verifichi lo scaricamento del flusso, il pacchetto che ha causato il danno ha già raggiunto la vittima. Pertanto, l'avviso o la perdita si verificano dopo che il pacchetto ha raggiunto la vittima. Questa azione viene eseguita quando il ACK della vittima per il pacchetto che ha causato il danno raggiunge l'IPS.



Informazioni sull'ispezione pre-ACK (normalizzazione del payload TCP/normalizzazione abilitata)

Questa funzione normalizza il traffico subito dopo la decodifica del pacchetto e prima dell'elaborazione di qualsiasi altra funzione Snort, in modo da ridurre al minimo le operazioni di evasione del TCP. Ciò garantisce che i pacchetti che raggiungono l'IPS siano gli stessi di quelli che vengono trasmessi alla vittima. Snort scarta il traffico sul pacchetto che completa l'attacco prima che l'attacco raggiunga la vittima.



Quando si abilita *Normalize TCP*, viene eliminato anche il traffico che soddisfa queste condizioni:

- Copie ritrasmesse di pacchetti ignorati in precedenza
- Traffico che tenta di continuare una sessione precedentemente eliminata
- Traffico che corrisponde a una di queste regole del preprocessore di flusso TCP:

  129:1129:3129:4129:6129:8129:11da 129:14 a 129:19

  Nota: Per abilitare gli avvisi per le regole di flusso TCP ignorate dal preprocessore di normalizzazione, è necessario abilitare la funzionalità *Anomalie di ispezione stateful* nella configurazione del flusso TCP.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).