IPS Application Manager 5.1 - tunnelhandtekeningen

Inhoud

Inleiding

Inbraakpreventiesysteem (IPS) 5.1 bevat meer dan 1000 ingebouwde standaardhandtekeningen. U kunt geen handtekeningen van de lijst van ingebouwde handtekeningen hernoemen of verwijderen, maar u kunt handtekeningen terugtrekken om ze uit de detectiemachine te verwijderen. U kunt later gepensioneerde handtekeningen activeren. Dit proces vereist echter dat de sensoren hun configuratie opnieuw uitbouwen, wat tijd vergt en de verwerking van het verkeer kan vertragen. U kunt ingebouwde handtekeningen afstemmen wanneer u verschillende signaturen aanpast. Ingebouwde handtekeningen die gewijzigd zijn, worden *afgestemde handtekeningen* genoemd.

Dit document illustreert de stappen die moeten worden gebruikt om de handtekening aan te passen met behulp van de IPS-apparaatbeheer (IDM). IDM is een op web gebaseerde, Java toepassing die u in staat stelt om uw sensor te configureren en te beheren. De webserver voor IDM bevindt zich op de sensor. U kunt deze functie benaderen via de webbrowsers Internet Explorer, Netscape of Mozilla.

Opmerking: U kunt handtekeningen maken, die *aangepaste handtekeningen* worden genoemd. Aangepaste signatuur-ID's beginnen bij 60000. U kunt ze voor verschillende dingen configureren, zoals het aanpassen van snaren op UDP-verbindingen, het volgen van netwerkoverstromingen en scans. Elke handtekening wordt gemaakt met behulp van een kenmerkende motor die speciaal is ontworpen voor het soort verkeer dat wordt bewaakt.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Inbraakpreventiesysteem Manager 5.x.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

Om een sensor te vormen om netwerkverkeer voor een bepaalde handtekening te controleren moet u de handtekening toelaten. Standaard worden de meest kritische handtekeningen ingeschakeld wanneer u de update voor handtekeningen installeert. Wanneer een aanval wordt gedetecteerd die overeenkomt met een enabled signatuur, genereert de Sensor een alarm, dat is opgeslagen in de gebeurtenis store van de Sensor. De waarschuwingen en andere gebeurtenissen kunnen van de eventwinkel worden opgeroepen door op het web gebaseerde klanten. De standaardinstelling is dat de Sensor alle informatieve waarschuwingen of hoger inlogt.

Sommige handtekeningen hebben onderhandtekeningen. De handtekening is onderverdeeld in subcategorieën. Wanneer u een sub-signatuur vormt, zijn wijzigingen die zijn aangebracht in de parameters van één sub-signatuur alleen van toepassing op die sub-signatuur. Bijvoorbeeld, als u handtekening 3050 sub-signatuur 1 bewerkt en de ernst wijzigt, is de ernst-verandering alleen van toepassing op sub-signatuur 1 en niet op 3050 2, 3050 3 en 3050 4.

Tune Signatures

Een pictogram + geeft aan dat er meer opties beschikbaar zijn voor deze parameter. Klik op het **+** pictogram om de sectie uit te vouwen en de resterende parameters te bekijken.

Een groen pictogram geeft aan dat de parameter momenteel de standaardwaarde gebruikt. Klik op het groene pictogram om deze in rood te veranderen, waarmee het veld parameter wordt geactiveerd, zodat u de waarde kunt bewerken.

Stap voor stap Procedure

Voltooi deze stappen om handtekeningen te stemmen:

1. Meld u aan bij IDM door gebruik te maken van een account met beheerder- of exploitatierechten.
2. Kies **Configuration > Signature Definition > Signature Configuration**.Het venster Signature Configuration verschijnt.
3. Kies een sorteeroptie uit de lijst **Door selecteren** om een handtekening te plaatsen.Als u bijvoorbeeld op zoek bent naar een UDP Flood signatuur, kies dan **L2/L3/L4 Protocol** en dan

UDP Overstromingen.Het deelvenster Signature Configuration frist zich op en toont alleen de handtekeningen die overeenkomen met uw sorteercriteria.

4. Selecteer de handtekening en vul de volgende stappen in om een bestaande handtekening aan te passen:Klik op **Bewerken** om het dialoogvenster Handtekening bewerken te openen.Controleer de parameter waarden en wijzig de waarde van een parameter die u wilt instellen.**N.B.:** Houd de **Ctrl**-toets ingedrukt om meer dan één eventactie te kiezen.Selecteer onder Status **ja** om de handtekening in te schakelen.**Opmerking:** de handtekening moet de sensor in staat stellen om de aanval actief te detecteren die door de handtekening wordt gespecificeerd.Specificeer onder Status of deze handtekening is ingetrokken. Klik op **Nee** om de handtekening te activeren. Dit plaatst de handtekening in de motor.**Opmerking:** Een handtekening moet worden geactiveerd zodat de sensor de door de handtekening gespecificeerde aanval actief kan detecteren.**N.B.:** Klik op **Annuleren** om de wijzigingen ongedaan te maken en het dialoogvenster Handtekening bewerken te sluiten.Klik op **OK**.De bewerkte handtekening verschijnt nu in de lijst met het type dat op Tuned is ingesteld.**Opmerking:** Als u de wijzigingen wilt opheffen, klikt u op **Terugzetten**.
5. Klik op **Toepassen** om uw wijzigingen toe te passen en de herziene configuratie op te slaan.

Gerelateerde informatie

- Cisco-inbraakpreventiesysteem
- Technische ondersteuning en documentatie – Cisco Systems