

整合 Cisco 主機安全管理軟體與 Cisco 入侵防禦系統

Cisco 主機安全管理軟體(Cisco Security Agent)與 Cisco 入侵防禦系統(Cisco Intrusion Prevention System, IPS)是 Cisco 威脅控制與封鎖策略中的兩大主軸，乃是 Cisco 自我防衛網路解決方案的基礎。Cisco Security Agent 可以辨識威脅並預防終端主機的惡意行為，為執行重要任務的伺服器與桌上型電腦，提供無可比擬的安全保護。可建置在不同平台上的 Cisco IPS，可以偵測、分類並即時阻止威脅發生，提供網路強大的防護功能。兩者結合起來，將可以建立一個真正點對點的威脅預防與封鎖解決方案，其所具備的防護功能將從核心網路基礎架構，一路延展到終端主機。

安裝在伺服器與桌上型電腦上的 Cisco Security Agent，對終端主機具有完整的能見度，讓 Cisco Security Agent 可以獲取網路上其他安全機制所看不到的資訊。Cisco Security Agent 與 Cisco IPS 強化偵測感應器的功能，以便利用這些寶貴的終端主機資訊。這樣的協同合作讓 Cisco IPS 提升對終端主機與整體網路潛在威脅的能見度，進而擴展整體威脅控制與封鎖的能力。

Cisco Security Agent 與 Cisco IPS 的結合，可提供下列效益：

- 利用 Cisco Security Agent 的終端主機資訊來協助 IPS 採取最適當的行動：利用終端主機的關聯性資料，Cisco IPS 可以確認網路威脅的嚴重程度，並指示網路採取適當的回應動作。
- 降低警報誤判(false positive)與未發警報(false negative)的機率：Cisco Security Agent 提供作業系統類型與其他終端主機狀態資訊，協助 Cisco IPS 確認威脅與網路的相關性，降低警報誤判與未發警報的機率。
- 加強化解攻擊的能力：Cisco IPS 可以運用 Cisco Security Agent 的觀察名單功能，協助提醒 Cisco IPS 關注被 Cisco Security Agent 認為是可疑或惡意的系統，並特別指出任何與這些系統有關的事件。
- 動態主機(host)隔離：Cisco IPS 可以動態封鎖被 Cisco Security Agent 認為具惡意的系統。這可將 Cisco Security Agent 的隔離功能擴充到 IPS。

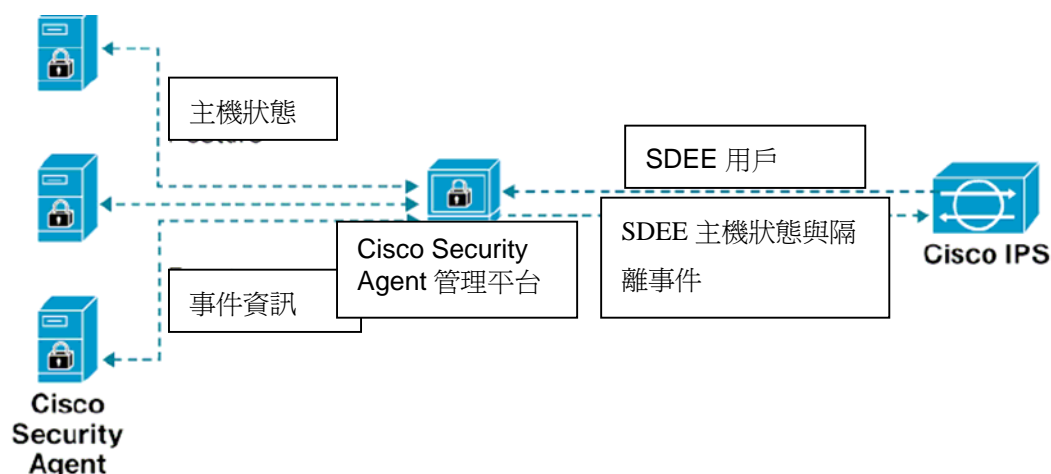
這份報告的主題是 Cisco Security Agent 與 Cisco IPS 的技術整合。它將描述這個協同機制如何運作，說明其好處並提供成功建置所需的準則。

Cisco Security Agent/Cisco IPS 協同合作架構

這個整合了 Cisco Security Agent 與 Cisco IPS 的架構，有賴三個主要元件的互動：

- Cisco IPS 偵測感應器：任何 Cisco IPS 平台至少都會建置 Cisco IPS 偵測器軟體 6.0 版，不是用 in line 的 IPS 模式就是用 IDS 模式的設定。
- Cisco Security Agent：以主機為基礎的 IPS 軟體，在需要被保護與監控的伺服器與桌上型電腦上執行。
- Cisco Security Agent 管理平台(CSA MC)：Cisco Security Agent 管理中心是一個獨立的軟體，提供 Cisco Security Agent 集中化安全政策的設定、監控、與管理功能。除此之外，CSA MC 會依據 Cisco Security Agent 發出的事件與狀態資訊，執行整體網路的關聯性確認工作。CSA MC 5.0 或是更新的版本，將需要與 IPS 整合。

圖一說明基礎架構中的這些元件與其互動關係。



圖一 Cisco Security Agent/Cisco IPS 協同合作架構

註：整合所需最基本的軟體版本，是 Cisco Security Agent 管理平台 5.0 版，與 Cisco IPS 軟體 6.0 版。

Cisco Security Agent 是一個以主機為主的管理機制，在應用軟體與作業系統核心之間運作，具備最高的終端主機能見度，提供執行重要任務的伺服器與桌上型電腦深度防禦的防護功能。Cisco Security Agent 的功能之一，就是發出寶貴的事件與狀態資訊，由 Cisco Security Agent 管理平台負責收集與進行關聯性分析。Agent 與 Cisco Security Agent 管理平台之間的檔案傳輸，則是透過 SSL 來保護。

除了從 Agent 處收集詳細的終端主機資訊之外，Cisco Security Agent 管理平台的整體網路關聯性分析所產出的威脅資料，也對 Cisco IPS 相當有價值。當這些資料分享給 Cisco IPS 時，可以協助提升 IPS 偵測感應器對終端主機與整體網路威脅的能見度。Cisco IPS 偵測感應器是利用安全設備事件交換(Secure Device Event Exchange；SDEE)協定來獲取這些資訊。SDEE 協定是由 Cisco 領導的協會所開發，是為了網路事件資訊的安全交換所設計的。Cisco Security Agent 管理平台與 IPS 之間的溝通，就是被 SSL/TLS 加密技術與 HTTP 認證技術所保護。

註：Cisco Security Agent 管理平台提供 X.509 憑證進行認證，而 IPS 偵測感應器則採用使用者名稱與密碼進行認證。

要開始接收資料時，IPS 偵測感應器需要向 Cisco Security Agent 管理平台定期存取 SDEE 協定。當溝通管道被認證與建立後，兩種型態的訊息就可以在 Cisco Security Agent 管理平台與 IPS 偵測感應器間相互交換：

- **Cisco Security Agent 狀態事件**：包括由 Cisco Security Agent 管理平台收集的主機狀態資訊，例如 IP 位址、與執行 Cisco Security Agent 主機所使用的作業系統種類。為了接收狀態事件的資訊，IPS 必須定期擷取 Cisco Security Agent 管理平台的資料。一旦擷取之後，Cisco Security Agent 管理平台會先寄一個先期狀態訊息，內含所有已知 Agent 的 IP 位址與作業系統種類。在這之後，Cisco Security Agent 管理平台會持續向 IPS 更新相關資訊。

- **隔離事件：** Cisco Security Agent 管理平台將向 IPS 偵測感應器溝通目前正在被隔離的主機清單。一個主機的隔離，可以透過 Cisco Security Agent 管理平台管理人員以人工執行，或是依整體網路關聯性規則而執行。隔離事件的資訊包括隔離原因、與違反規定的相關協定(例如 TCP、UDP、ICMP 等)、說明是否違反規定的隔離是與既有的 TCP 連結還是 UDP 有關的參數、被隔離主機的 IP 位址等。IPS 偵測感應器必須先擷取相關資訊，才能收到隔離事件訊息。Cisco Security Agent 管理平台將先送出初期狀態訊息，列出所有被隔離的主機，並陸續更新之後的隔離事件。

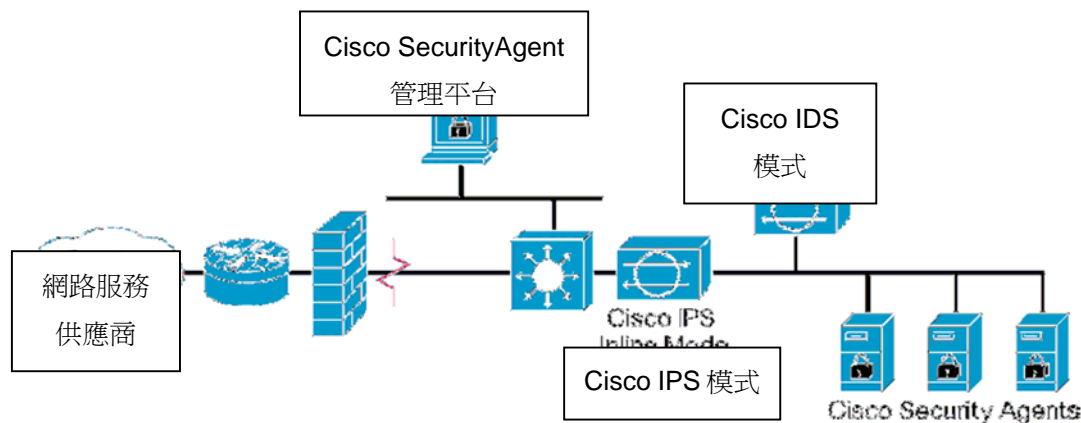
建置考量

一般來說，把 Cisco Security Agent 與 Cisco IPS 建置在同樣環境中的最佳作法，同這兩個解決方案各自單獨建置的最佳做法一樣。因此，只要有可能，遵循這些最佳做法。除了採用 Cisco Security Agent 與 Cisco IPS 規劃的最佳做法之外，在整合兩個產品時還有其他一些需要指出的考量因素：

IPS 與 IDS 模式

Cisco Security Agent 可以與設定在 IPS 模式或是 IDS 模式的 Cisco IPS 偵測感應器整合。這將可帶來更大的彈性，因為網管人員可會因不同的原因，而必須決定採用某種 IPS 模式。

即便可能有許多不同的設計，一個採內部保護模式建置的典型 IPS，將是介於 Cisco Security Agent 與網路其它部分中間。這樣的話，當惡意的封包通過系統時，IPS 便可以動態封鎖威脅。在一個典型的 IDS 模式建置中，IDS 將會連上一個設定用來擷取主機流量的交換埠，而這些主機則是受到 Cisco Security Agent 的保護。圖二中，可以看到三種不同的設計。



圖二 IPS/IDS 典型的建置設計

一個 Cisco Security Agent 管理平台對多個 IPS 偵測感應器

單一的 Cisco Security Agent 管理平台可以同時服務多個 IPS 偵測感應器。在 IPS 偵測感應器由不同部門管理員分開管理時，他們進入 Cisco Security Agent 管理平台的管道可以依據不同存取憑證而分開。

一個 IPS 偵測感應器對兩個 Cisco Security Agent 管理平台

一個偵測感應器可以設定最多與兩個 Cisco Security Agent 管理平台同時互動。除了為了有備援的重要目的之外，這個功能還可以簡化 Cisco Security Agent 管理平台最新版本的升級流程。

虛擬化

Cisco Security Agent 可以與設定為虛擬偵測感應器的 IPS 整合。當使用這樣的虛擬化功能時，所有 Cisco Security Agent 管理平台提供的資料對 IPS 偵測感應器來說，都將是包含整體網路的資料，因此可以被所有運作中的虛擬偵測感應器使用。

IP 位址

Cisco Security Agent 管理平台與 IPS 偵測感應器，都是依據 IP 位址來辦認主機。因此，這兩個機制對於 IP 位址空間應該有一致性的看法。將 Cisco Security Agent 管理平台與 IPS 偵測感應器建置在網路轉址技術(Network Address Translation, NAT)許多不同網段，可能導致兩個機制的位址空間不相容。因此，IPS 偵測感應器可能無法與 Cisco Security Agent 管理平台提供的資訊相符。一個主機可能被 Cisco Security Agent 管理平台與 IPS 偵測感應器視為是兩個不同的系統，或是兩個分開的系統被誤認為是一個系統。在所有的狀況下，不相容的位址空間，會降低整合品質，並極為可能導致在錯誤的主機上，採取化解威脅的行動。

通常最佳作法，是在任何可能狀況下，避免將 NAT 建置在 Cisco Security Agent、Cisco Security Agent 管理平台與 IPS 偵測感應器之間。當需要建置 NAT 時，要注意將 Cisco Security Agent 管理平台與 IPS 偵測感應器放在 NAT 的同一區段，確保這兩個產品有同樣的 IP 位址空間能見度。

Cisco Security Agent/Cisco IPS 介面設定

將 Cisco Security Agent 與 Cisco IPS 整合在一起，需要設定 Cisco Security Agent 管理平台與 IPS 偵測感應器。在大部分的情況下，有以下三種主要的設定動：

1. 定義 IPS 偵測感應器在擷取 SDEE 時使用的 Cisco Security Agent 管理平台之管理帳號。
2. 在每個 IPS 偵測感應器中，將 Cisco Security Agent 管理平台設定為被信任的主機。
3. 設定每個 IPS 偵測感應器中的外部產品介面定義。

定義 Cisco Security Agent 管理平台管理帳號

Cisco Security Agent 與 IPS 之間的溝通是被認證過的；事實上，除非提出要求的 IPS 偵測感應器成功通過認證，否則 Cisco Security Agent 管理平台將不會接受一個為了瞭解狀態與隔離訊息的 SDEE 擷取要求。為了這個目的，每個 IPS 偵測感應器需事先設定一個有效 Cisco Security Agent 管理平台帳號的使用者名稱與密碼，獲得最基本的閱覽權限。當 IPS 偵測感應器提出存取請求時，就會提供 Cisco Security Agent 管理平台這個認證訊息，而 Cisco Security Agent 管理平台則可以依據這些認證訊息可信度，以決定接受或拒絕存取請求。

即便企業可以利用任何既存、具有基本閱覽權限的 Cisco Security Agent 管理平台管理帳號，我們並不建議這樣的做法。基於明顯的安全考量，開啟一個全新的專屬帳號以負責 Cisco Security Agent 與 IPS 之間的溝通，永遠都是比較好的做法。這個帳號不能具備超過最基本所需的權限(監控、閱覽等)。

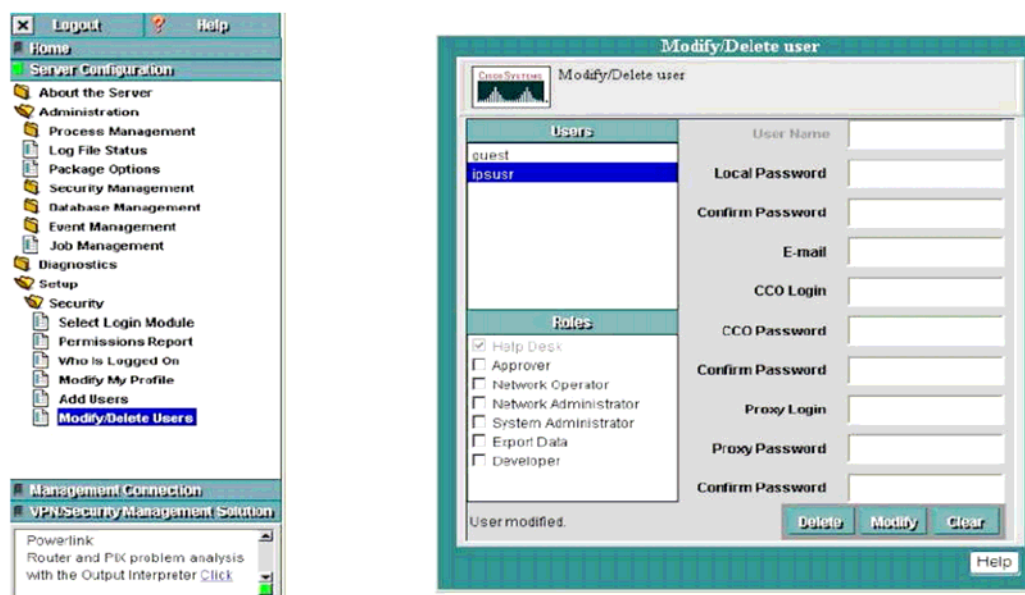
在同一個管理人員下與有多個 IPS 偵測感應器的環境中，單一帳號可以被所有系統分享，但是在所有 IPS 偵測感應器不是被同一個管理人員管理的環境中，可以定義多個帳號來區隔不同的管理人員。

在 Cisco Security Agent 管理平台 5.0 版中，管理帳號是設定在 Cisco 虛擬私有網路/安全管理解決方案(CiscoWorks VPN/Security Management Solution ; VMS)中，這是因為 Cisco Security Agent 管理平台 5.0 版以及更早之前的版本，是 CiscoWorks VMS 的元件之一。Cisco Security Agent 管理平台 5.1 版及之後的版本，這些帳號將可獨立存在，不需要有 VMS。在這些較新的版本中，被用來進行 Cisco Security Agent 管理平台與 IPS 之間溝通的帳號，可從 Cisco Security Agent 管理平台直接定義。

用於進行 Cisco Security Agent 管理平台與 IPS 之間溝通的帳號，理想上的設定應該具備監控權限，這表示使用者可以閱讀 Cisco Security Agent 資料庫的全部資料，但是沒有撰寫權限。在 Cisco Security Agent 管理平台 5.1 版及之後的版本中，這個監控角色可以被設定在 Cisco Security Agent 管理平台中，成為使用者設定的一部份。在 Cisco Security Agent 管理平台 5.0 版及之前的版本中，是由 VMS 而非 Cisco Security Agent 管理平台來定義管理使用者。在這樣的狀況下，使用者可以與任何已事先被 CiscoWorks 定義好的角色連結，但是僅具有閱讀的權限。以「Help Desk」為例，網管人員、系統管理人員、與系統作業員的角色，都具備撰寫權限，因此，針對 Cisco Security Agent 管理平台與 IPS 之間的溝通，就不建議採用上述人員的權限。

圖三是 Cisco Security Agent 管理平台 5.0 版的一個快照，說明「ipsusr」帳號的定義，乃是為了專門進行 Cisco Security Agent 與 IPS 之間的溝通。

圖三 Cisco Security Agent 管理平台管理帳號



想要了解更多關於管理帳號的訊息，請參照您的 Cisco Security Agent 管理平台相關文件。

將「Cisco Security Agent 管理平台系統」設定為被信任的主機

Cisco IPS 提供一串與其溝通的所有被信任的主機清單，包括封鎖設備、TLS/SSL 伺服器、與外部設備，例如 Cisco Security Agent 管理平台等。這個清單包含被 IPS 使用的被信任系統的數位憑證資料，以俾建立安全的連線。

執行 Cisco Security Agent 管理平台的系統也需要成為被信任的主機，這是 Cisco Security Agent 管理平台/IPS 介面設定的一部份。在加入這些系統的過程中，IPS 可以得到 Cisco Security Agent 管理平台的數位憑證資料，公開其系統特徵(fingerprint)，然後提交給網管人員批准。當網管人員批准相關的 fingerprint 後，Cisco Security Agent 管理平台系統就成為被信任的主機。

圖四是 Cisco IPS Device Manager (IDM) 6.0 版的一個快照，顯示主機 172.16.3.3(執行 Cisco Security Agent 管理平台的系統)，已經被列為被信任的主機。

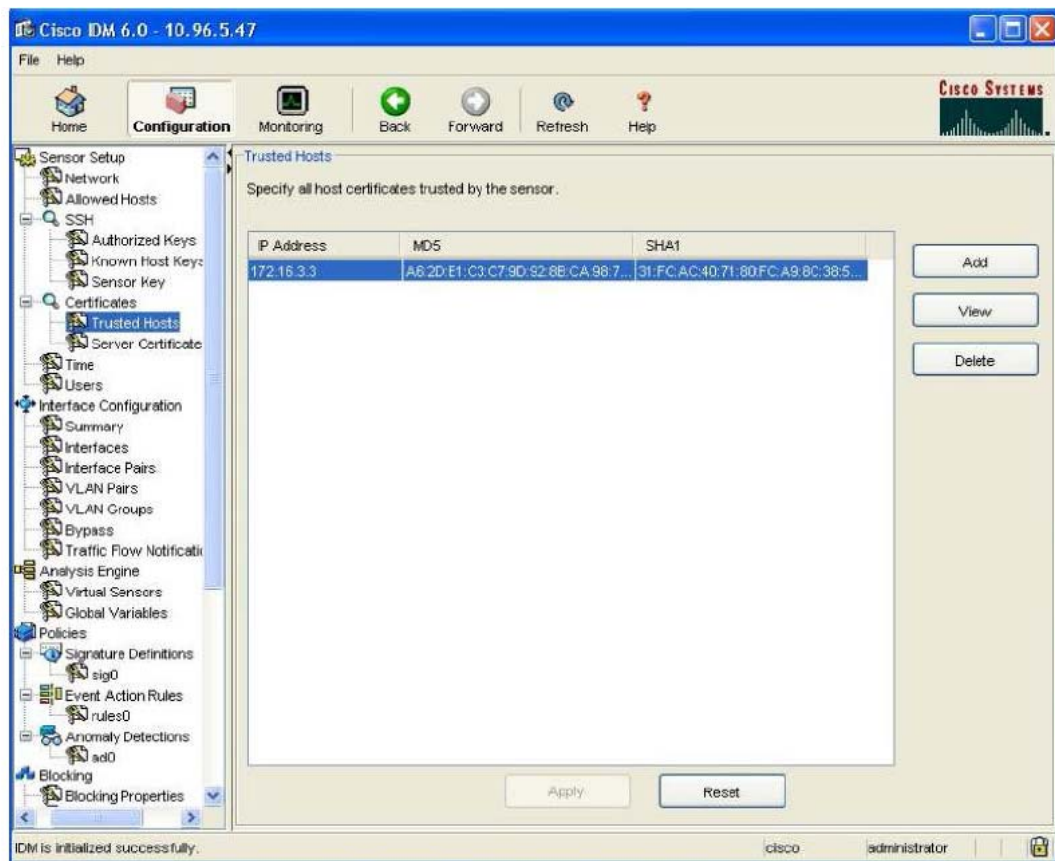
圖四 IPS 信任的主機

設定 IPS 外部產品的介面

Cisco IPS 偵測感應器具備一個外部產品的介面，設計用來處理外部安全與管理產品的溝通，例如 Cisco Security Agent 管理平台。多虧了這個介面，IPS 偵測感應器得以充分利用由 Cisco Security Agent 管理平台所維護的那些主機狀態與威脅狀況的有用資訊，包括被 Cisco Security Agent 所保護的系統之作業系統種類、與疑似出現惡意活動的系統之 IP 位址清單。這個等級的協同合作，有效提升了 Cisco Security Agent/IPS 點對點安全解決方案的整體安全度。

註：在 Cisco IPS 偵測感應器軟體 6.0 版中，只定義了兩個外部產品介面。Cisco Security Agent 管理平台是其目前唯一支援的外部產品。

IPS 外部產品介面的設定，包括定義溝通參數、觀察清單設定、與主機狀況設定等(見圖五)



圖五 IPS 外部產品介面設定

以下是外部產品介面設定中的所有參數解釋。

General Parameters (一般性參數)

External Product's IP Address : Cisco Security Agent管理平台所在主機系統的IP位址。

Enable Receipt of Information : 啟動/關閉外部產品介面。

Communication Settings (通訊參數) 定義通訊參數

SDEE URL : 確定將與 Cisco Security Agent 管理平台溝通的 URL。系統將提供原始設定的 SDEE URL。但是要注意，SDEE URL 可能必須依不同 Cisco Security Agent 管理平台版本，而有所更動。

Port : 用於通訊的埠口。原始設定埠口是 443。

Use TLS : 指出安全 TLS 通訊已經啟動。通訊將一直被 TLS 保護，這個參數是不能更改的。

Logging Settings (登錄設定)

在與 Cisco Security Agent 管理平台的溝通中，設定使用者名稱與密碼。

Username : 管理帳號的使用者名稱是用來與 Cisco Security Agent 管理平台進行溝通。

這個帳號是由 Cisco Security Agent 管理平台所定義。

Password/Confirm Password : 管理帳號的密碼是用來與 Cisco Security Agent 管理平台進行溝通。

Watch List Settings (觀察名單設定)

這個部分的設定,是用來啟動或關閉觀察名單的接收。它同時定義出在風險評估(Risk Rating)應該被提升的參數值。這份報告稍後將詳細討論觀察名單如何運作。

Enable Receipt of Watch List : 啟動/關閉 Cisco Security Agent 管理平台提供之觀察名單的接收。

Manual Watch List RR Increase : 指明升高風險評估(Risk Rating)的增加數值。針對手動加入觀察名單的主機有關的安全事件,風險評估應該升高。根據原始設定,這個參數值為 25,但是這個數值可以在 0 到 35 之間。

Session-Based Watch List RR Increase : 指明升高風險評估的增加數值。由於 Cisco Security Agent 整體網路關聯性的功能,針對與加入觀察名單的 TCP 連結有關之安全事件,風險評估應該升高。根據原始設定,這個參數值為 25,但是這個數值可以在 0 到 35 之間。

Packet-Based Watch List RR Increase : 指明升高風險評估的增加數值。由於 Cisco Security Agent 整體網路關聯性的功能,針對與加入觀察名單的 UDP 多層協定有關之安全事件,風險評估應該升高。根據原始設定,這個參數值為 10,但是這個數值可以在 0 到 35 之間。

Host Posture Settings (主機狀態設定) 界定應該如何處理主機狀態資訊。

Enable Receipt of Host Postures : 啟動/關閉 Cisco Security Agent 管理平台提供之主機狀態資訊的接收。

Allow Unreachable Hosts' Postures : 允許/拒絕來自 Cisco Security Agent 管理平台無法接觸到的主機之狀態訊息接收。當在過濾 IP 位址無法被 IPS 辨識或可能在網路中被複製的主機訊息時,這樣的功能選項特別有用。

Posture ACLs : 根據原始設定,所有的主機狀態訊息都是經由 IPS 所處理。狀態 ACLs 提供一個機制,可以過濾網路範圍,在其中主機狀態訊息會被處理或忽視(許可或是拒絕)。當在過濾 IP 位址無法被 IPS 辨識或可能在網路中被複製的主機訊息時,這樣的功能選項特別有用。

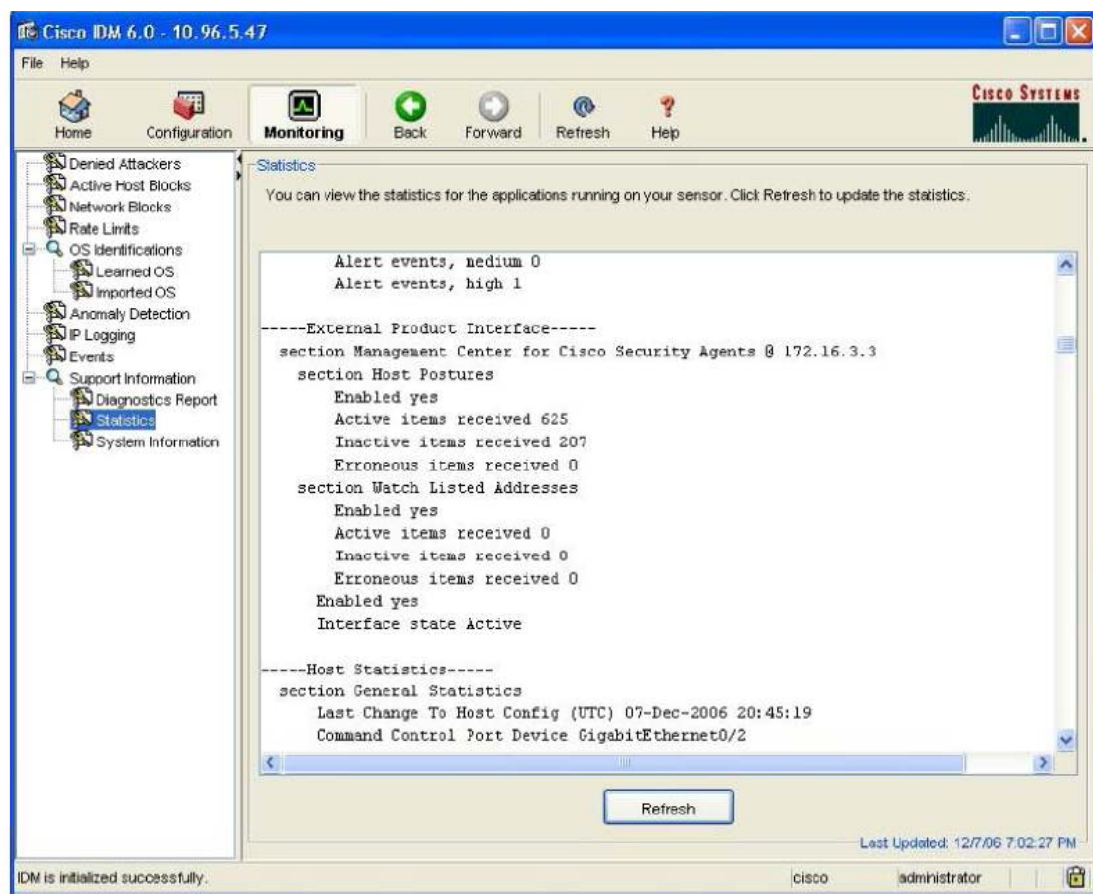
驗證外部產品介面的狀態

為了驗證在 IDM 中外部產品介面的狀態,您可以進入 Monitor/Statistics(監控/統計)部分,如圖六所示。在正常的狀況下,介面狀態應該是 Active。若是出現「Communications Failed」(溝通失敗)的狀況,有可能是因為錯誤的使用者名稱或是密碼,或是使用者不具備足夠的閱覽權限,或是因為 IPS 偵測感應器無法連結上 Cisco Security Agent 管理平台。

圖六是 IDM6.0 版統計頁的一個快照。上面的數字表示主機 172.16.3.3 與 Cisco Security

Agent 管理平台的溝通是 Active 的。

圖六 驗證外部產品介面的狀態



使用終端主機資訊

Cisco Security Agent 與 Cisco IPS 整合的優勢之一，就是可讓 IPS 偵測感應器使用 Cisco Security Agent 認證過的作業系統種類資訊。這樣的資訊將可以擴充 IPS 對終端主機的能見度，協助做出更聰明的決策，並進而降低警報誤判(false positive)與未發警報(false negative)的可能性。

所謂警報誤判(false positive)，是指 IPS 啟動警報以回應某些活動，但是這些活動實際上並不具備惡意威脅，或者是 IPS 的回應動作，與問題嚴重度不成比例。相反的，所謂未發警報(false negative)，是指 IPS 沒有針對真正惡意活動，發出警報或採取任何適當的回應行動。當 IPS 無法判斷某網路事件的風險程度時，警報誤判與未發警報的問題就會經常發生。利用 Cisco Security Agent 提供的作業系統種類資訊，Cisco IPS 能更佳的適當確認某一特定事件相關的風險度，降低報誤判與未發警報發生的可能性。

從 Cisco IPS 偵測感應器軟體 5.0 版開始，IPS 警報會被一個先進的風險評估機制衡量。每個 IPS 警報都會被量化為從 0 到 100 的數值，這就被稱做風險評估(Risk Rating)，可以讓使用者了解網路在啟動警報的事件下，面臨了多大的風險。實際上，風險評估要不是用在偵測感應器設定為 IDS 模式下，以特別指出那些需要立即處理的事件，就是用在偵測感應器被設定為 IPS 模式下，以啟動回應動作。

當與 Cisco Security Agent 整合時，Cisco IPS 可以依據 Cisco Security Agent 提供之作業系統種類訊息，來動態調整風險評估值，以確認某一事件的正確風險程度。這樣的話，當被鎖定的作業系統類型並不脆弱時，IPS 可以調降風險嚴重度。但當作業系統類型很脆弱時，IPS 可以調升風險嚴重度。

以下的部分將討論如何計算出風險評估值，以及 Cisco Security Agent 提供的資訊會對風險評估計算造成甚麼影響。

IPS 風險評估計算

Cisco IPS 5.0 最先導入的風險評估機制，將 IPS 偵測感應器啟動的警報所代表的風險量化表示。風險評估是以 0 到 100 的數值表示，數值愈高，就表示啟動警報的事件之風險愈高。風險評估的計算，考慮整合了多種因素，包括受攻擊網路之資產價值、攻擊的真實度、威脅的嚴重度、以及其他重要的關聯性因素。自 Cisco IPS 偵測感應器軟體 6.0 版開始，風險評估的計算將被加強，增加兩項新的因素：Promiscuous Delta，這個因素考慮到偵測感應器設定的模式；以及觀察名單評比(Watch List Rating)，其乃採用 Cisco Security Agent 提供的觀察名單。

$$\text{Risk Rating} = \frac{\text{Fidelity(SFR)} \star \text{Severity(ASR)} \star \text{Target Value(TVR)}}{100 \star 100 \star 100} + \text{Relevancy(ARR)} - \text{Promiscuous Delta(PD)} + \text{Watch List(WLR)}$$

攻擊特徵真實性評估(Signature Fidelity Rating, SFR)：由 Cisco 事先定義，並可以依每個特徵而重新設定更改。以特定規則(特定規律表達)寫的特徵值，比用一般性規則而寫的特徵值，SFR 要來的高。可接受的數值介於 1 與 100 之間。

警報嚴重性評估(Alert Severity Rating, ASR)：由 Cisco 事先定義，並可以依每個特徵而重新設定更改。這個數值是跟一個成功攻擊的嚴重性相關。可能的數值包括：

- **訊息(25)**—一個訊息警報是網路交通流量中常見的警報，在大多數的網路上，沒有特別的安全相關性問題。可能只是違反一些網路政策，但是一般來說都不會對網路安全造成立即危險。
- **低嚴重性(50)**—一個低嚴重性的警報，也是通常出現在良性網路交通流量中，但是在某些網路上卻可能不尋常。類似像網路管理設備常見的公開掃描，也被歸類屬於低嚴重性的警報。雖然這種掃描可能是攻擊的前驅，一個公開掃描成為攻擊的目的來卻屬少見。
- **中度嚴重(75)**—一個中度嚴重的警報，一般出現在網路上不會看到的交通流量中。通常都是屬於中級程度的偵查流量、針對自我復原服務的阻斷服務(Denial-of-Service, DoS)攻擊、意外訊息或是計畫的遠端存取等。這種行為需要調查或是預防性動作，有時甚至需要使用者做出政策決定。
- **高嚴重度(100)**—一個高嚴重度的警報，出現在可以指出主動攻擊或明顯攻擊前身的交通流量中。正常的網路應該不會見到這樣的交通流量。這個評估保留給可能會對目標造成嚴重傷害的攻擊，以及那種只在秘密偵查交通流量中可見到的網路交通。

目標資產價值評估(Target Value Rating, TVR)：可以依不同目標資產進行設定。

這是目標資產被認定價值的權重值。原始設定給予所有目標中級價值。這使得使用者可以升高與關鍵系統相關聯事件的風險程度，也可以降低低價值系統事件的風險程度。可能的價值數值包括：

- 低資產價值 (75)
- 中級資產價值(100)
- 高級資產價值(100)
- 重要任務資產價值(200)

攻擊相關性評估(Attack Relevancy Rating, ARR)：這是個內部權重值，計算方式乃是依目標與 IP 所知或是從 Cisco Security Agent 匯入的威脅關聯性資訊。ARR 值代表特定目標對於攻擊的脆弱度：

- ARR 是 10 的話，表示目標系統的作業系統被認定屬於脆弱。這適用於 IDS 與 兩種模式。
- ARR 是-10 的話，表示目標系統的作業系統不被認定屬於脆弱，而 IPS 則是設定在 IDS 模式。
- ARR 是 0 的話，表示目標系統的作業系統不被認定為屬於脆弱，而 IPS 則是設定在 IPS 模式。

註：目標的作業系統，不是 IPS 透過系統特徵，就是從 Cisco Security Agent 匯入的資訊得知。因此，Cisco Security Agent 提供的終端主機資訊，會影響 ARR 數值。

Promiscuous Delta (PD)：Promiscuous Delta 是 Cisco IPS 偵測感應器軟體 6.0 版首度推出的功能，是由 Cisco 依據特徵性而事先定義好的數值，其目標是降低於 IDS 模式中發出的特定警報之風險評估。這個正數數值，可以從 0 到 30。

Promiscuous Delta 是當一個系統在 IDS 模式時，每當發出一個警報時，就從風險評估中扣減而算出。一般來說，在內部保護模式的系統，對於目標主機有比較清楚界定的圖像，而其所發出的警報也會比 IDS 模式系統所發出的要來的精確。

那些無明確服務、作業系統或是應用的特徵值(signature)，其原始設定都沒有 Promiscuous Delta(PD=0)。那些服務、作業系統或是應用明確的特徵值，則是設定為 Promiscuous Delta5、10、15，其計算方式是從每個種類扣除 5 而算出。

註：雖然每個 PD 值可以依據特徵值進行設定，但是我們並不建議您自行更改 Promiscuous Delta 中的預設值。

觀察名單評估(Watch List Rating, WLR)：觀察名單評估是 Cisco IPS 偵測感應器軟體 6.0 版首度推出的功能，將會提升與 Cisco Security Agent 觀察名單中的系統，與其相關事件之風險評估值。觀察名單評估乃由外部產品介面軟體所設定，包含三個主要指標，數值在 0 到 35 之間：

- **Manual Watch List(手動觀察名單)RR 值增加：**指明升高風險評估(Risk Rating)的增加值。針對手動加入觀察名單的主機有關的安全事件，風險評估應該升高。根據原始設定，這個增加值為 25。
- **Session-based Watch List(多層協定觀察名單)RR 值增加：**指明升高風險評估的增加值。由於 Cisco Security Agent 整體網路關聯性的功能，針對與加入觀

察名單的 TCP 連結有關之安全事件，風險評估應該升高。根據原始設定，這個增加值為 25。

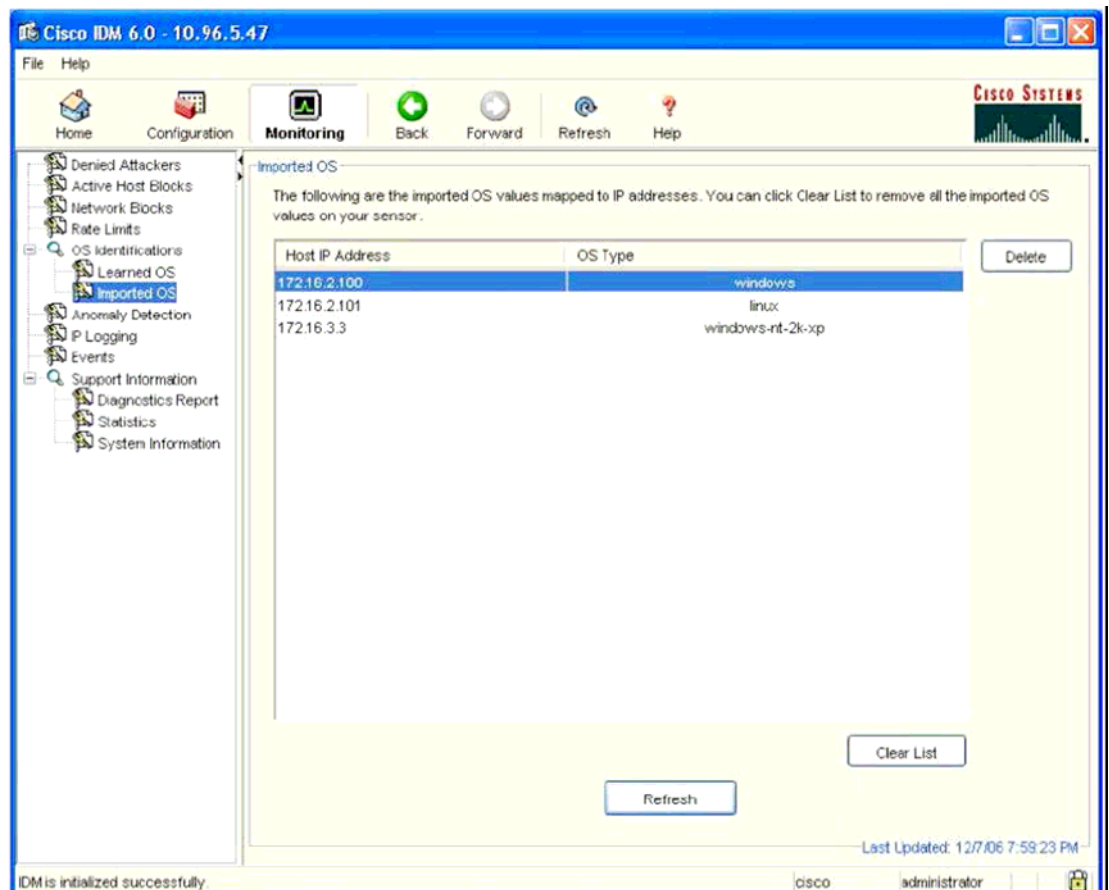
- **Packet-based Watch List(封包觀察名單)RR 值增加：**指明升高風險評估的增加值。由於 Cisco Security Agent 整體網路關聯性的功能，針對與加入觀察名單的 UDP 多層協定有關之安全事件，風險評估應該升高。根據原始設定，這個增加值為 10。

驗證匯入作業系統狀態資訊

如前所述，Cisco Security Agent 提供之作業系統種類訊息，在計算風險評估(RR)時扮演重要角色。為了驗證 IPS 是否已經成功匯入 Cisco Security Agent 提供之作業系統種類訊息，可以利用 IDM 「Monitoring」 (監控) 部分「Imported OS」 (OS 匯入) 的標識(tab)。

圖七是匯入 IP 位址的清單，以及與其相對應的作業系統類型。

圖七 匯入作業系統資訊



使用 Cisco Security Agent Watch Lists

Cisco Security Agent 的功能之一，就是隔離違反安全規定或出現惡意行為的主機。導致主機隔離的發生，可能是由於多個 Cisco Security Agent 發出的安全事件，經動態的整體網路關聯性分析之結果；要不然就是網管人員手動設定隔離。當主機被隔離時，該主機的 IP 位址會被加入隔離 IP 清單中，而所有執行 Cisco Security Agent 的系統，將會封鎖所有與被感染主機之間的溝通嘗試。

為了更高的威脅能見度與整體控制，IPS 外部產品介面可以設定使用 Cisco Security Agent 提供的隔離訊息。這樣的話，每當 Cisco Security Agent 隔離一台主機時，就會發出隔離事件訊息，給接收隔離訊息的每個 IPS 偵測感應器。隔離事件訊息包括隔離原因、與違反規定相關的協定 (TCP、UDP、ICMP 等)、與隔離主機的 IP 位址。

有了 Cisco Security Agent 提供的隔離訊息，每個 IPS 偵測感應器皆可以建立並維護一個觀察名單。觀察名單的目的是為了協助 IPS 監控被 Cisco Security Agent 認為是可疑或惡意的系統，並提醒注意任何與這些系統有關的事件。觀察名單將會告訴 IPS 哪些系統需要仔細監控，而哪些系統的風險評估必須被提高。事實上，IPS 並不會只因為一台主機出現在這個名單上就封鎖它。

註：對一台主機來說，名列觀察名單上表示將被 Cisco Security Agent 隔離，並被 IPS 觀察。但是 IPS 並不會自動隔離觀察名單上的系統。

每當觀察名單上的主機發出警報時，觀察名單評估就會因此將風險評估提高。如前所述，觀察名單的評估是在 IPS 外部產品介面中所設定。這些不同數值的界定，以區隔手動與動態隔離，以及 TCP 和 UDP 交通流量。IPS 會根據特定事件的狀況，採用相對應的觀察名單評估類型。

由於這樣的觀察名單，一個在名單上的主機啟動之事件的風險評估，會自動增高。還有另外一個功能設定選項。當一個具攻擊力的系統的風險評估超過預先設定的門檻時，便可以採取覆蓋回應行動(override action)來封鎖這個系統。本文稍後將會討論這種概念。

將主機加入觀察名單

一個主機可以透過 Cisco Security Agent 的網管人員手動設定，或是依據 Cisco Security Agent 的整體網路關聯性計算的結果，被加入觀察名單：

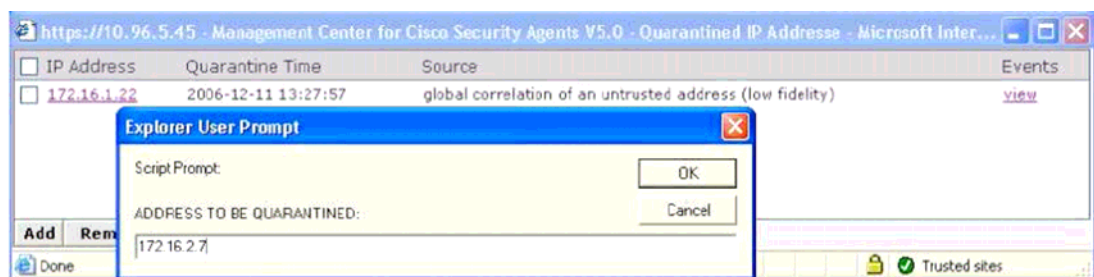
手動設定

Cisco Security Agent 網管人員可以選擇用手動設定，隔離被感染的系統，或是那些為了特定理由必須隔離在網路之外的系統。

要手動隔離主機，網管人員必須把主機的 IP 位址加入隔離 IP 位址清單。作法是在 Cisco Security Agent 管理平台的「Global Event Correlation」(整體網路事件關聯性) 部份中，進入「dynamically quarantined IP addresses」(動態隔離 IP 位址)連結，然後加入欲隔離主機的 IP 位址。

圖八說明這個隔離流程。在這個例子中，IP 位址是 172.16.2.7 的系統被手動加入隔離清單中。

圖八 手動將主機加入隔離清單中

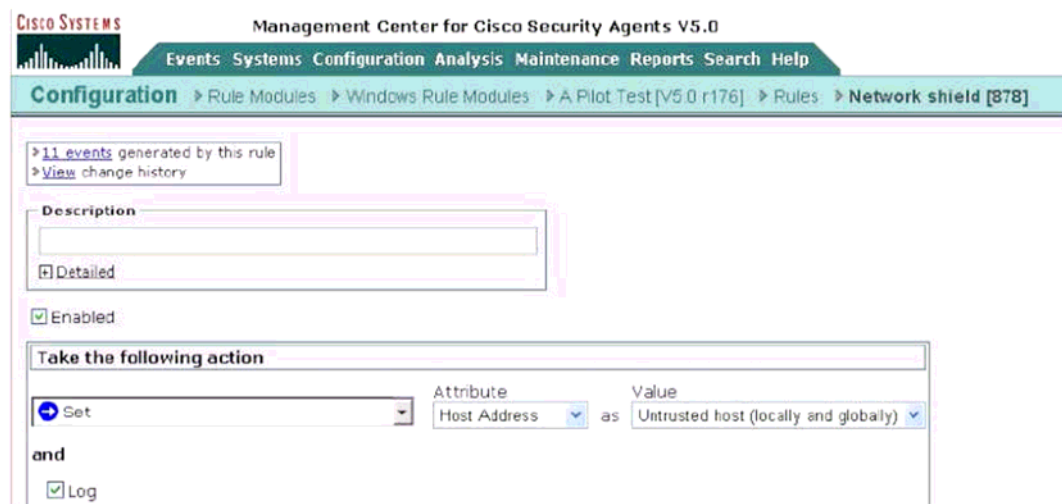


手動將主機加入隔離 IP 位址清單中時，會發出隔離事件訊息給 IPS 偵測感應器。除了將受感染系統的 IP 位址加入清單外，隔離事件訊息還會說明這是利用手動加入。因此，IPS 將會在計算風險評估時，利用手動觀察名單 RR 增加數值。

Dynamic Global Correlation (動態整體網路關聯性)

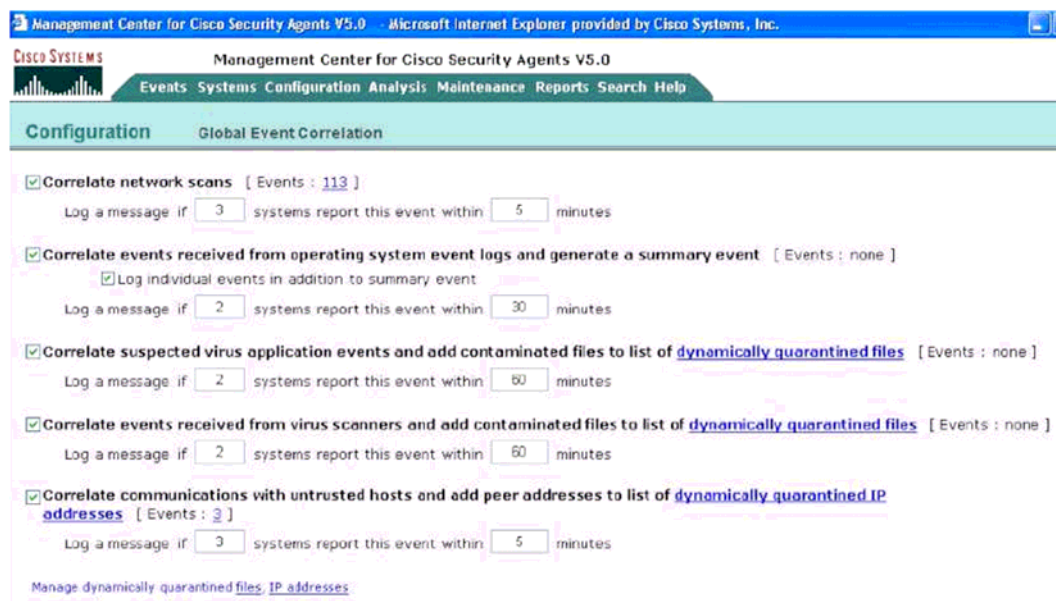
當主機違反安全規則、與未受信任之主機溝通、或是出現惡意行為時，Cisco Security Agent 便可以動態隔離這些主機。這種動態設定需要有一個規則，將該攻擊性主機界定為整體網路皆不信任的主機，並啟動該事件的網路整體關聯性。

驅動隔離的規則，必須將主機位址設定為不受信任的主機(對局部網路與整體網路皆然)，以回應規則違反的行為。被設定為不受信任的主機(對局部網路與整體網路皆然)時，該主機就成為整體網路事件關聯性之標的物。圖九對此狀況做出說明。



圖九 將攻擊性主機設定為整體網路皆不信任的規則

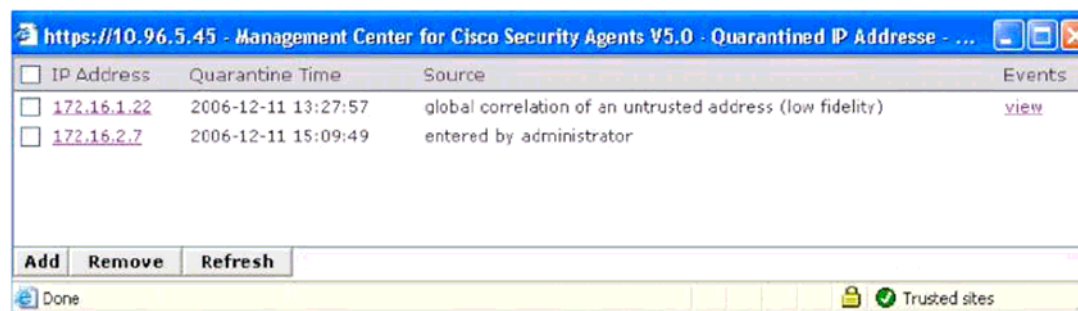
在設定這樣的規則後，Cisco Security Agent 必須設定可以與不受信任之主機進行關聯性溝通，並將其位址加入動態隔離 IP 位址清單中。這個設定包括一個事件門檻的定義，在覆蓋此門檻後，主機就會自動被加入所有執行 Cisco Security Agent 的系統之整體網路隔離名單。



圖十是整體網路事件關聯性的設定說明。

每當一個系統被隔離時，一個隔離事件訊息就會被送到 IPS 偵測感應器，這些訊息包括隔離主機的 IP 位址、相關的協定、並會說明隔離事件的動態本質。因此，當在計算風險評估時，IPS 必須利用兩種動態觀察名單評估值(多層協定或是封包式)。

舉例來說，圖十一是隔離 IP 位址的清單。這個清單上包括一個由於整體網路關聯性而被隔離的系統(172.16.1.22)，以及一個被網管人員手動加入的系統(17.16.2.7)。



圖十一 隔離 IP 位址的清單

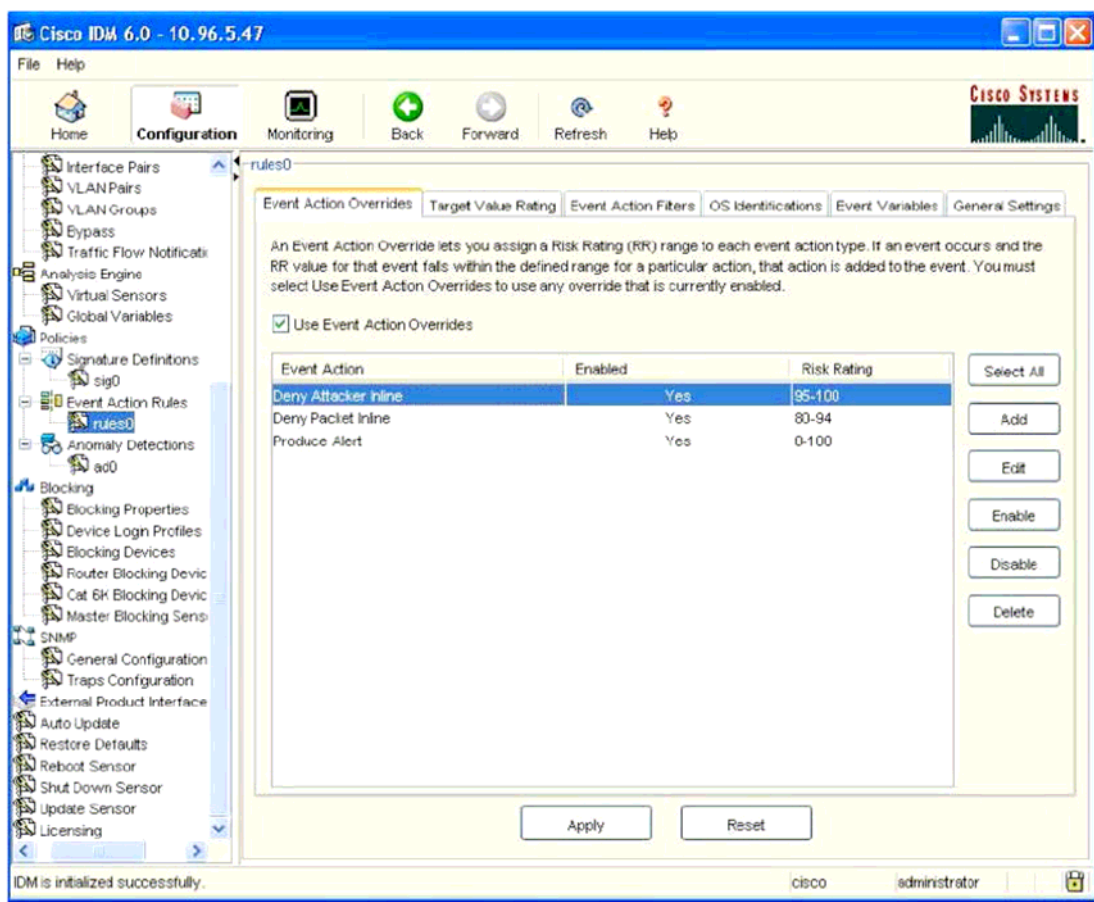
IPS Event Action Override (IPS 事件覆蓋回應行動)

如前所述，Cisco IPS 導入觀察名單主要是為了提醒注意可疑系統的活動。雖然 Cisco Security Agent 會隔離在清單中的主機，但是 IPS 本身並不會自動執行隔離。然而，還是有可能將觀察名單與一個或多個「事件覆蓋回應行動」 (Event Action Override) 結合，以動態封鎖清單中的主機。

「事件覆蓋回應行動」是指一個一般性規則，會對風險評估落入特定範圍的事件，做出回應動作，而其回應程度已經覆蓋攻擊特徵 (signature) 層級所界定的回應動作。由於觀察名單之故，IPS 會升高在名單中系統所造成事件之風險評估。一個「事件覆蓋回應行動」之設定，在一個主機造成的事件已經超越預設的風險門檻時，網路便可以封鎖該攻擊性主機。

當系統設定在內部保護模式(IPS)時，「事件覆蓋回應行動」的設定就應可以在線上封鎖攻擊者；當系統設定為 IDS 模式時，就應該可以封鎖主機，避免主機與網路連結。

圖十二是這些概念的說明。



圖十二 「事件覆蓋回應行動」範例

在圖十二中，有三種「事件覆蓋回應行動」，提供給設定在 inline 模式的 IPS。風險評估報為 95 或更高的網路事件，會讓事件源頭的主機被 IPS 在網上封鎖。而啟動的警報之風險評估在 80 到 94 之間的封包，也將會在線上被動態拒絕。最後，任何風險評估在 0 到 100 之間的事件，都將會在登錄日誌(log)中引發警報。

「事件覆蓋回應行動」的建置，會是有用的工具，可以將 Cisco Security Agent 執行的主機

隔離，拓展到 IPS，創造一個真正的點對點，從終端主機到網路的作法。雖然這個做法有明顯的好處，在採用之前還是有某些面向必須考量：

- 一旦設定了「事件覆蓋回應行動」，它將會適用於所有風險評估落在設定範圍中的安全事件，而不光只是那些跟觀察名單中主機有關的事件。
- 在觀察名單內的主機引發事件的風險評估，落在「事件覆蓋回應行動」明定的範圍內之前，IPS 將不會採取任何行動。這表示當 IPS 從 Cisco Security Agent 管理平台接收到隔離事件訊息時，它並不會立即隔離主機。只有當主機在 IPS 端發動一個事件時，它才會對主機採取行動。

相關文件

依字母順序排列

- Cisco IPS 風險評估

http://www.cisco.com/en/US/products/hw/vpndevc/products_white_paper0900aecd80191021.s.html

- 安裝與使用 Cisco Intrusion Prevention System Device Manager 6.0

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_configuration_guide_book09186a00807a8a2a.html

- 使用 Management Center for Cisco Security Agent 5.0

http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_book09186a00805ae89c.html

- 使用 Management Center for Cisco Security Agent 5.1

http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_book09186a008067b6a5.html



台北總公司
台北市信義路四段 460 號 12 樓
www.cisco.com.tw
Tel: 02 - 8758 - 7100
Fax: 02 - 8758 - 7199

台中辦事處
台中市公益路二段 51 號 20 樓 A2
www.cisco.com.tw
Tel: 04 - 2327 - 1372

高雄辦事處
高雄市苓雅區三多四路 110 號 19 樓之 2
www.cisco.com.tw
Tel: 07 - 338 - 1092
Fax: 07 - 338 - 1094

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 ©2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco System Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609F)