安全參考資訊

有關產品安全事件響應團隊(PSIRT)提供的其他資訊，請參閱http://www.cisco.com/go/psirt。

最佳實踐

提高Cisco路由器的安全性

本檔案是一些思科組態設定之非正式討論，網路管理員應考慮在路由器（尤其是邊界路由器）上變更這些設定，以提高安全性。本文檔介紹基本的「樣板」配置項，這些項幾乎普遍適用於IP網路，並且介紹您應該瞭解的幾項意外項。

Cisco IOS 密碼加密須知

某個思科以外的來源公佈了一項計畫，要解密思科組態檔中的使用者密碼（和其他密碼）。該計畫並不能使用 enable secret 指令來解密密碼組。此計畫在思科客戶間引發疑慮的程度出乎意料，因此我們不禁懷疑，許多客戶對思科密碼加密提供之安全性的仰賴程度，似乎超出了原先設計的範圍。本檔案將說明思科密碼加密背後的安全模式，以及加密的安全限制

思科的安全藍圖

SAFE是一個全面的安全藍圖，使組織能夠安全地開展電子商務。SAFE採用模組化方法，可隨著網路的增長和變化而簡化安全設計、部署和管理，從而增強基於Cisco AVVID（語音、影片和整合資料架構）的網路。

攻擊防禦、跟蹤或緩解策略

使用Cisco路由器識別和跟蹤資料包泛洪

> 拒絕服務(DoS)攻擊在Internet上很常見。對此類攻擊作出響應的第一步是查明攻擊的確切型別。許多常用的DoS攻擊都基於高頻寬資料包泛洪或其他重複的資料包流。本文檔提供瞭解和跟蹤這些攻擊的資訊。

[與尼姆達病毒作鬥爭的戰略]

該指數提供了處理Nimda病毒的所有技術提示和緩解建議的綜合清單。

[紅色代碼蠕蟲的防治策略]

此索引提供處理「紅色代碼」蠕蟲的所有技術提示和緩解建議的綜合清單。

[防禦分散式拒絕服務(DDoS)攻擊的策略]

本白皮書包含有關潛在DDoS攻擊如何發生的技術說明，以及使用Cisco IOS軟體防禦該攻擊的建議方法。

[防止UDP診斷埠拒絕服務攻擊的策略]

本白皮書包含有關潛在UDP診斷埠攻擊發生的技術說明，以及使用Cisco IOS軟體防禦該攻擊的建議方法。

[防止TCP SYN拒絕服務攻擊的策略]

本白皮書包含有關潛在TCP SYN攻擊如何發生的技術說明，以及使用Cisco IOS軟體防禦該攻擊的建議方法。

[最新的拒絕服務攻擊：「精簡」描述和資訊，以儘量減少影響]
注意：上面的連結指向不由Cisco Systems， Inc.維護的外部站點。

它提供有關「smurf」攻擊的深入資訊，重點介紹Cisco路由器以及如何減少這些攻擊的影響。某些資訊是一般資訊，與組織選擇的特定供應商無關；但編寫時以思科路由器為中心。本文檔並未確認「smurf」攻擊對其他供應商裝置的影響；但本文檔中確實包含有關不同供應商的資訊。

其他資源

[思科產品安全事件回應]

本檔案介紹錯誤報告和事件回應程式 — 具體來說，如果您受到主動安全攻擊，或您相信您將受到攻擊，如果您思科產品存在安全問題，如果您想取得思科產品的技術安全資訊，或如果您對某個思科產品已宣佈的安全問題有其他疑問，該怎麼做。說明思科產品安全事件響應團隊(PSIRT)在處理安全事件中的作用。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。