

効果的なファイヤーウォールの設定

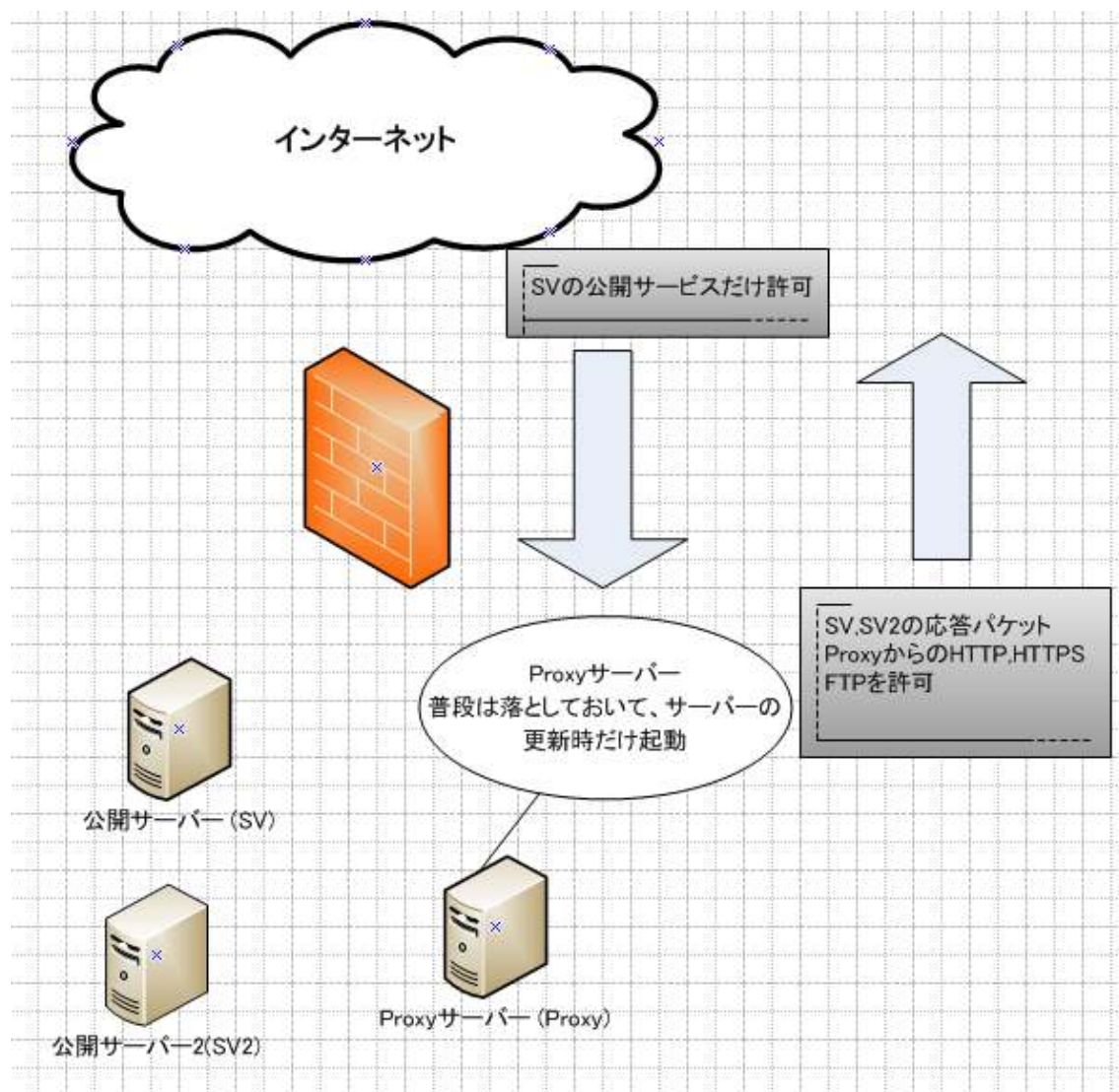
バッファオーバーフロー系の攻撃は、おもに C や C++ でかかれたプログラムのバウンダリチェック漏れをもとにして攻撃します。

オーバーフローさせた後に、短い攻撃コードを送り込んで外部から本体のプログラムをダウンロードさせてコンピューターを乗っ取ります。

これに対抗するためには `libsafe` や `stack randomization` などが考えられます

これは直接的にバッファオーバーフローを防ぐという考え方です

一方ここで述べる設定は、本体のプログラムを外部からダウンロードさせないことを主眼とします。



上記の設定によって、SV,SV2 からの外部へのアクセスが遮断されるため、悪意あるプログラムのダウンロードを防ぐことができます。

また、セキュリティパッチなどは、Proxy 経由で取得できるため運用上の問題も起きません

これは非常に効果のある設定で、実際にゼロデイ exploit が出回ったとしても、攻撃者は本体である悪意あるプログラムを SV または SV2 に送ることができなくなるため、外部への迷惑行動や、サーバー内での不当な行動がとりにくくなります。

2008/10/10

碓 永志

ikari@ecoin.jp