セグメンテーションとネットワーク仮想化技術を使用した安全なイントラネットの構成方法の提案と検証

Proposal and Evaluation of a Secure Intranet Architecture Using Segmentation and Network Virtualization Technologies

武内弾・ネットワーク分科会・情報セキュリティ大学院大学

In recent years, there has been a steady stream of information leaks due to targeted attacks that move laterally, such as ransomware. Large-scale networks are strengthening network security by incorporating network virtualization, segmentation, and the zero trust concept. Security issues within intranets have long been discussed, but the recent influx of attacks suggests that the current situation has not improved. This study proposes a secure intranet configuration method that protects intranet resources from cyberattacks that move laterally, such as ransomware. By setting up segments and controlling access between them, access to unauthorized segments is blocked. Access control was achieved by introducing network virtualization technology (OpenStack Neutron) to the network server. To address concerns about overloading the network server's routing process, an experimental intranet environment was implemented and evaluated, confirming the validity of the above proposal.

1.研究背景

- 近年ランサムウェアの被害は広がっている。
- 令和6年度の日本国内のサイバー攻撃の被害のうち、「ランサムウェアによる業務影響」が「電子メールの不正中継（不正送信）」と並んで最も高い
- ランサムウェアはネットワーク間を横移動する性質を持っている
- イントラネットは昔から信頼されたネットワークとして運用されている傾向
- エンドポイントセキュリティや外部から内部を守るセキュリティはあるものの、イントラネット内部そのもののセキュリティ対策がほぼない

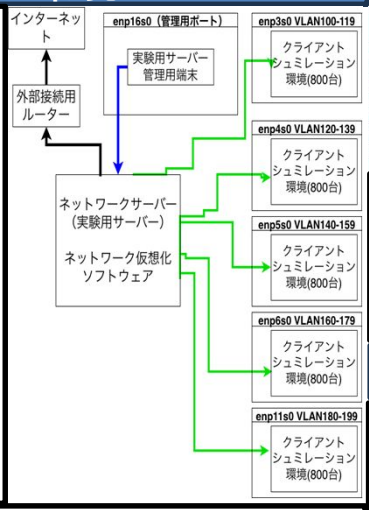
2.提案内容

- 横移動を防止する為の適切なアクセス制御が必要
- リソース毎にアクセス制御を行うには動的アクセス制御とマイクロセグメンテーションが必要

- (今回の取り組み)ネットワークサーバにネットワーク仮想化ソフトウェアを導入してアクセス制御を実現
- (残課題)マイクロセグメンテーションでユーザ情報や認証結果等で判断を行う動的アクセス制御を行う場合は，アイデンティティ・ガバナンス・プログラム（IGP）が必要になる

3.検証環境

- ネットワークサーバーは中小規模の環境で最小限の構成で測定するため、コンシューマCPUを搭載した環境
- クライアントシュミレーション環境ではクライアントにはLinux OSを搭載
- 物理 NIC 上に VLAN サブインターフェースを生成し，さらに Macvlan デバイスを作成して Network Namespace へ割り当てる構成
- クライアント端末は合計 5 台用意し，各クライアントが 担当範囲となる 20 個の VLAN セグメントを生成



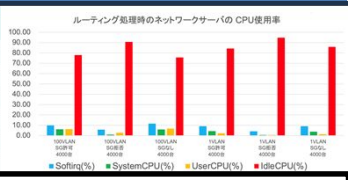
- 攻撃地点となりサーバ内に実在する各セグメントの負荷受信ポートを強制的にリンクアップ状態にしてSGを設定し，受信方向（Ingress）にのみACLが適用されている状態

4.測定方法

- 手段
  - セグメンテーションが機能している環境で負荷をかけて、ルーティング処理やSGによるアクセス制御が過負荷状態にならず正常に行えているか確認
- 実験
  - 4000台（フロー）分の端末から1秒毎に100PPSのパケットをSGによるアクセス制御が行われているサーバー内の特定のポート群に送信
  - パケットを投げる際はSGによってアクセスが許可されたポート、不許可のポートの2つに許可されたポートに投げる際にSGの設定を切った3種類で測定
- 評価手法
  - 4000台からのアクセスが発生している状態でネットワーク仮想化ソフトウェアのプロセスの使用率とCPUアイドルの残量を分析することで、限られた計算リソースにおけるネットワーク仮想化ソフトウェアの実行可能性を評価した。
- 攻撃方法
  - mausezahn を使用.
  - パケットは1台に付き100PPSを1秒ごとに出力.
  - 理由としてはncやiperf3を使用すると正規の接続をクライアント側に維持しようとするが，それを行うとクライアント側がパンク．セグメントとSGの有無による受信時のルーティング処理時の負荷測定とした。

5.結果

Label	PPS_RX	PPS_TX	Softirq(%)	System CPU (%)	User CPU (%)	Idle CPU (%)	Conntrack (Sever)
100VLAN_SG許可_4000台	405193.29	1007.02	9.77	6.07	6.28	77.86	4000.00
100VLAN_SG拒否_4000台	404039.71	598.33	5.69	0.94	2.66	90.63	0.00
100VLAN_SGなし_4000台	408816.79	982.10	11.63	5.94	6.76	75.64	4000.00
1VLAN_SG許可_4000台	410435.15	38.60	9.16	4.37	2.15	84.29	4000.00
1VLAN_SG拒否_4000台	408303.58	0.00	4.08	0.55	0.60	94.70	0.00
1VLAN_SGなし_4000台	410505.46	33.81	9.04	3.81	1.23	85.89	3999.96



- SGでアクセスが拒否されている時はConntrackが0でアクセス制御による遮断が正常に行われている。
- 100セグメント環境でSG許可はアイドル78%、SG拒否はアイドル90%(ACLでドロップした後のルーティング処理がないため)
- セグメント1つ（L2通信時）の場合とセグメント100個の場合ではセグメント数が多い方が負荷が若干あがる。(複雑なL3ルーティング処理の影響)

6.まとめ

- 100個のセグメント環境でルーティング処理中のCPUの負荷は22%で78%ほど余裕があった
- ネットワーク機能に限定する事で中小規模な環境でもネットワーク仮想化ソフトウェアでイントラネットを構築する事が可能である事を示した。
- 一方、ユーザ認証等によるマイクロセグメンテーションでのアクセス制御の実装や送信時も含めたルーティング処理量 の測定、通常通信時 の負荷計測など課題もあった。