VisualFirewall: A Firewall Visualization Tool for Network Management and Security Analysis

Chris Lee, Jason Trost, Nick Gibbs, Raheem Beyah, John A. Copeland
Why do we need VisualFirewall?

- Analyzing network traffic and IDS alerts in textual form is a tedious task that lacks a high-level view of activity.
- Passive-monitoring.
- VisualFirewall provides a visualization tool to teach networking concepts.
- It is difficult to verify firewall configurations.
- Multiple simultaneous views makes visualization attacks much more difficult.

Chris Lee - http://www.csc.gatech.edu/
What is VisualFireWall?

Realtime Traffic View

Realtime Signature Statistics

IDS Alarms
What is VisualFirewall?

Visual Signature View

Realtime

Signature

Statistics

IDS Alarms
What is VisualFirewall?
What is VisualFirewall?
Why Multiple Views?

• Temporality
  – Each view has a different effective time window and level of detail

• Malviz prevention (Greg Conti)
  – An visualization attack must now attack 3 to 4 different visualizations at the same time.

• Information multidimensionality
  – Different views can represent different dimensions of information.

Chris Lee - http://www.csc.gatech.edu/
Conclusion

• Designed for passive, real-time monitoring.
• Multiple views makes visualization attacks (malviz) difficult.
• Simple visualization of accept and rejection of packets. Useful for testing firewalls.
• Initial comments are promising, but needs usability testing.

Chris Lee - http://www.csc.gatech.edu/
Nmap Port Scan
Distributed Denial of Service
Bittorrent Traffic
Bittorrent Traffic
Bittorrent Traffic