Effectiveness of Application Identification in Next-Generation Firewalls

Christian Tsirlis, Brad Wilson
Advisor: Jorge Crichigno

Department of Integrated Information Technology
University of South Carolina

April 22nd, 2021

Agenda

- Purpose
- Introduction
- Problem description
- Background information
  - Next-generation Firewalls (NGFWs) and how they compare to traditional firewalls
  - Application Identification
- Proposed solution and implementation
- Conclusion

Purpose

- Understand Application Identification
- Understand Security Policy rules
- Implement Application Identification in Security Policies
- Protect network from outside attackers by analyzing traffic traversing the network
- Build stronger policies to minimize attacks

Introduction

- An application is a program or feature whose traffic can be labeled and monitored.

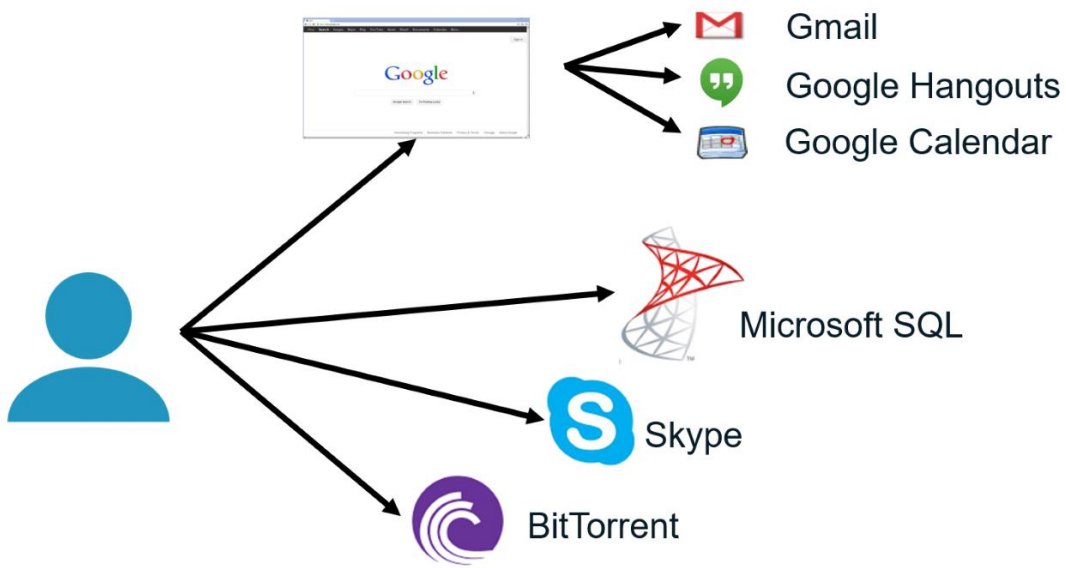


Figure 1. Example of Applications and their sub-applications

Problem Description

- Suspected malicious activity from Internet attempting to access internal network
- Evasive applications from Internet trying to enter internal network
- Effectiveness of security policies using Application Identification to protect internal network

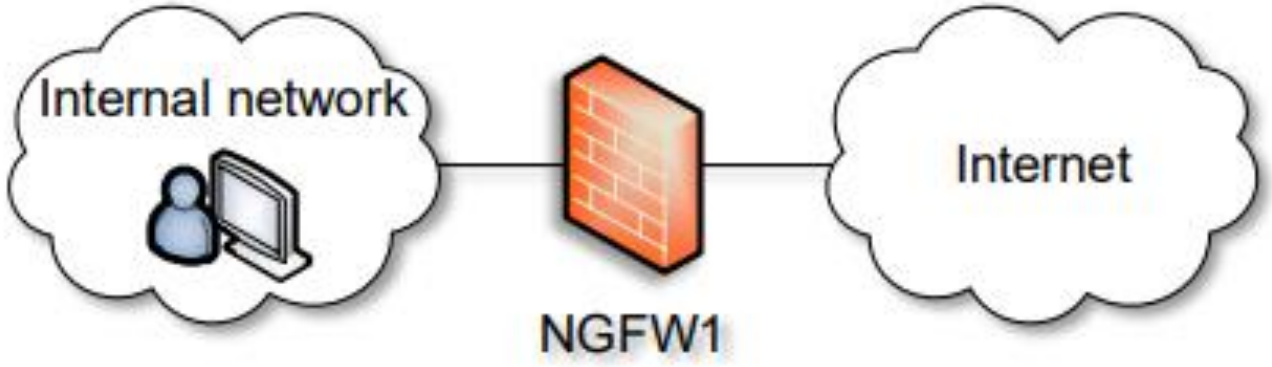


Figure 2. Network Topology

Background Information

- Traditional Firewalls
  - Identify traffic by IP address, port and protocol
  - Create holes which can be exploited by attackers
- Application Identification
  - Identifies traffic by application
  - Helps detect applications that evade traditional firewall

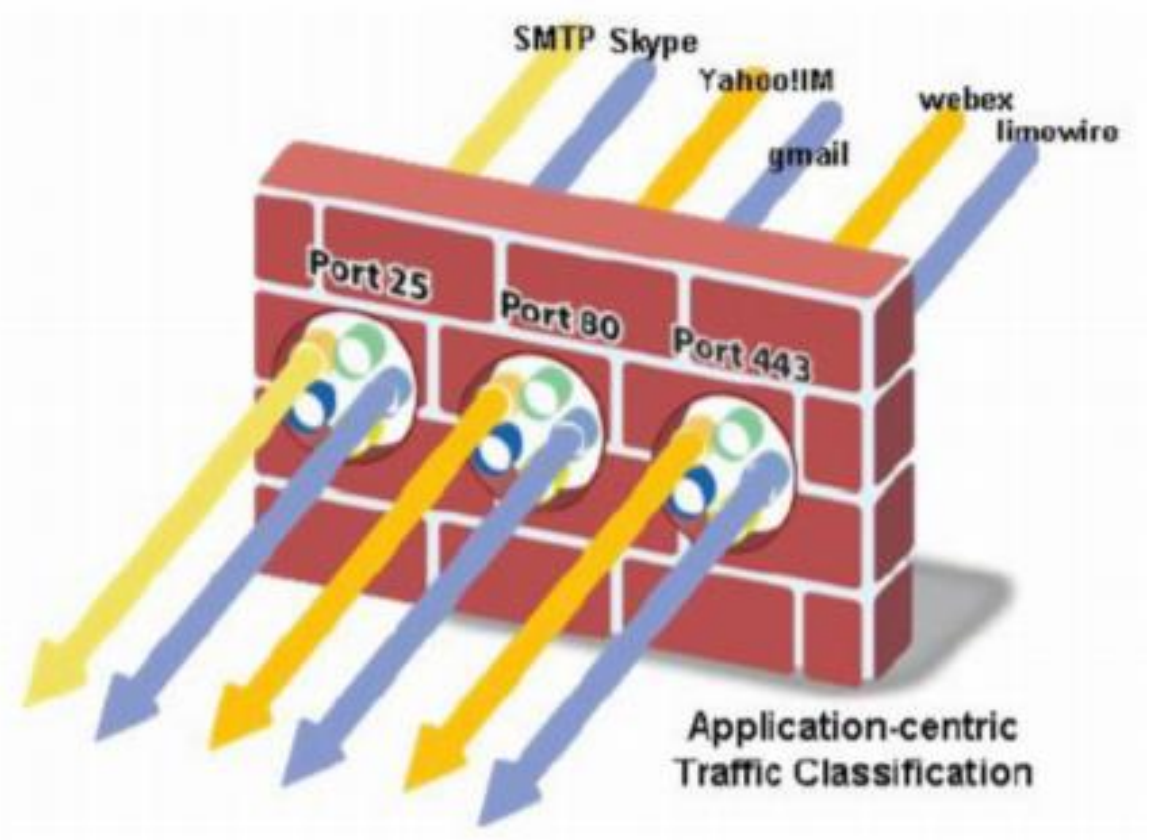


Figure 3. Shows how applications can enter a Traditional firewall

Proposed Solution and Implementation

- Application Identification was used to analyze Skype application

		Source	Destination			
	Name	Zone	Zone	Application	Service	Action
1	Block-Skype-Internal-Internet	internal network	internet	skype	application-default	Deny
2	Allow-internal-internet	internal network	internet	any	application-default	Allow
3	intrazone-default	any	(intrazone)	any	any	Allow
4	interzone-default	any	any	any	any	Deny

Figure 4. Security Policy for Application Identification using Skype

- Results
  - Skype uses numerous IP destination addresses to connect
  - Security policy blocks any file sharing and chat messages
  - Security policy fails to block audio/video calls

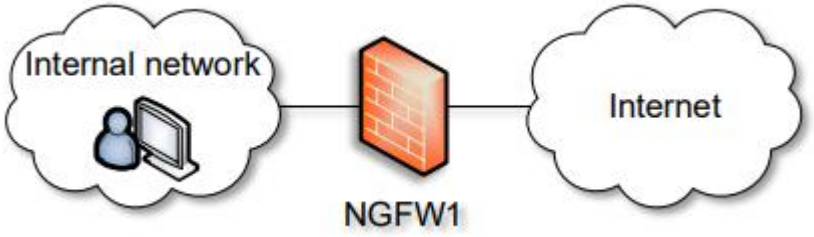


Figure 2. Network Topology

Analyzing Skype Data

		Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule
		04/12 19:23:35	deny	internal network	internet	192.168.1.20	20.185.212....	443	skype	deny	Block-Skype-Internal-Internet
		04/12 19:23:35	deny	internal network	internet	192.168.1.20	20.185.212....	443	skype	deny	Block-Skype-Internal-Internet
		04/12 19:23:22	deny	internal network	internet	192.168.1.20	13.88.31.235	443	skype	deny	Block-Skype-Internal-Internet
		04/12 19:21:26	deny	internal network	internet	192.168.1.20	20.185.212....	443	skype	deny	Block-Skype-Internal-Internet
		04/12 19:21:26	deny	internal network	internet	192.168.1.20	20.185.212....	443	skype	deny	Block-Skype-Internal-Internet
		04/12 19:21:26	deny	internal network	internet	192.168.1.20	20.185.212....	443	skype	deny	Block-Skype-Internal-Internet
		04/12 19:21:14	deny	internal network	internet	192.168.1.20	40.86.187.166	443	skype	deny	Block-Skype-Internal-Internet
		04/12 19:20:16	deny	internal network	internet	192.168.1.20	20.185.212....	443	skype	deny	Block-Skype-Internal-Internet
		04/12 19:20:12	deny	internal network	internet	192.168.1.20	20.185.212....	443	skype	deny	Block-Skype-Internal-Internet
		04/12 19:19:49	deny	internal network	internet	192.168.1.20	40.86.187.166	443	skype	deny	Block-Skype-Internal-Internet
		04/12 19:18:58	deny	internal network	internet	192.168.1.20	40.87.19.190	443	skype	deny	Block-Skype-Internal-Internet
		04/12 19:18:48	deny	internal network	internet	192.168.1.20	20.185.212....	443	skype	deny	Block-Skype-Internal-Internet
		04/12 19:18:46	deny	internal network	internet	192.168.1.20	20.185.212....	443	skype	deny	Block-Skype-Internal-Internet
		04/12 19:18:29	deny	internal network	internet	192.168.1.20	13.83.65.43	443	skype	deny	Block-Skype-Internal-Internet
		04/12 19:18:21	deny	internal network	internet	192.168.1.20	40.87.19.190	443	skype	deny	Block-Skype-Internal-Internet
		04/12 19:18:15	deny	internal network	internet	192.168.1.20	13.83.65.43	443	skype	deny	Block-Skype-Internal-Internet
		04/12 19:18:12	deny	internal network	internet	192.168.1.20	13.83.65.43	443	skype	deny	Block-Skype-Internal-Internet
		04/12 19:18:06	deny	internal network	internet	192.168.1.20	13.83.65.43	443	skype	deny	Block-Skype-Internal-Internet
		04/12 19:18:05	deny	internal network	internet	192.168.1.20	13.83.65.43	443	skype	deny	Block-Skype-Internal-Internet

Figure 5. Monitor logs showing numerous IP destination addresses

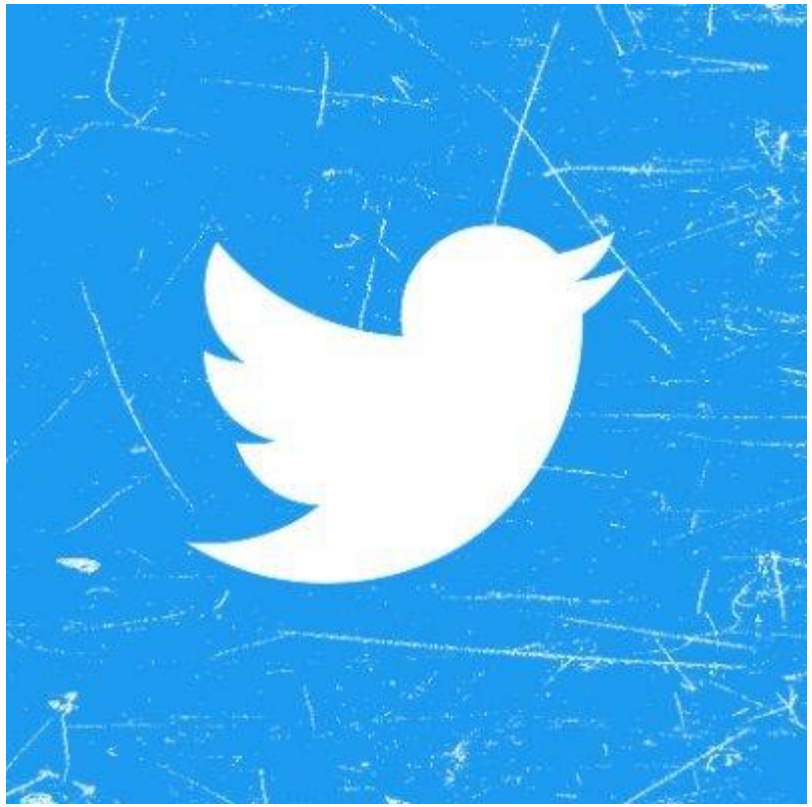
Twitter Results

Twitter-base

- Blocking this application was successful
- Example
  - Could not access twitter at all

Twitter-posting

- Blocking this application was unsuccessful
- Examples
  - Could like tweets
  - Could comment on tweets
  - Could retweet



Twitter Data

Manual Help

(rule eq 'twitt')

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule
	04/15 00:56:36	deny	inside	outside	192.168.1.20		104.244.42.193	443	twitter-base	reset-both	twitt
	04/15 00:56:35	deny	inside	outside	192.168.1.20		104.244.42.193	443	twitter-base	reset-both	twitt

Conclusion

- Why is this work important?
  - Our test highlights, that there are some weaknesses in Application Identification and how applications are evolving and finding a way to evade firewalls.
- Future work includes deeper packet analysis
- Questions?
- Thank you for listening and watching