Arizona State University
Center for Cybersecurity and Digital Forensics
781 Terrace Road, 4th Floor
Tempe, AZ 85281

iSecure Protector Server Edition with Biometric Signature and 5-Factor Authentication Validation Project

Objective

Determine the effectiveness of iSecure Protector Server Edition in protecting critical servers from external and internal attacks and the efficiency in bandwidth cost savings and productivities that iSecure Protector Server Edition provides.

Environment

1. Amazon AWS EC2 Instance running Windows Server 2016.
    a. ec2-18-216-115-95.us-east-2.compute.amazonaws.com
    b. IP Address: 18.216.115.95
    c. * Username: Administrator
    d. * Password: crX.4@=W*eaRdlcv$lWj?ieLqlF)YJ7i

    * Username and Password was disclosed during the second phase of the test and iSecure Protector Server Edition was in protection mode.

2. iSign iSecure Protector Server Edition Management Portal
    a. https://www.isignapps.com/iSecureProtector2017/SE
    b. Username: isecureprotector
    c. Password is the administrator's biometric signature

Initial Setup

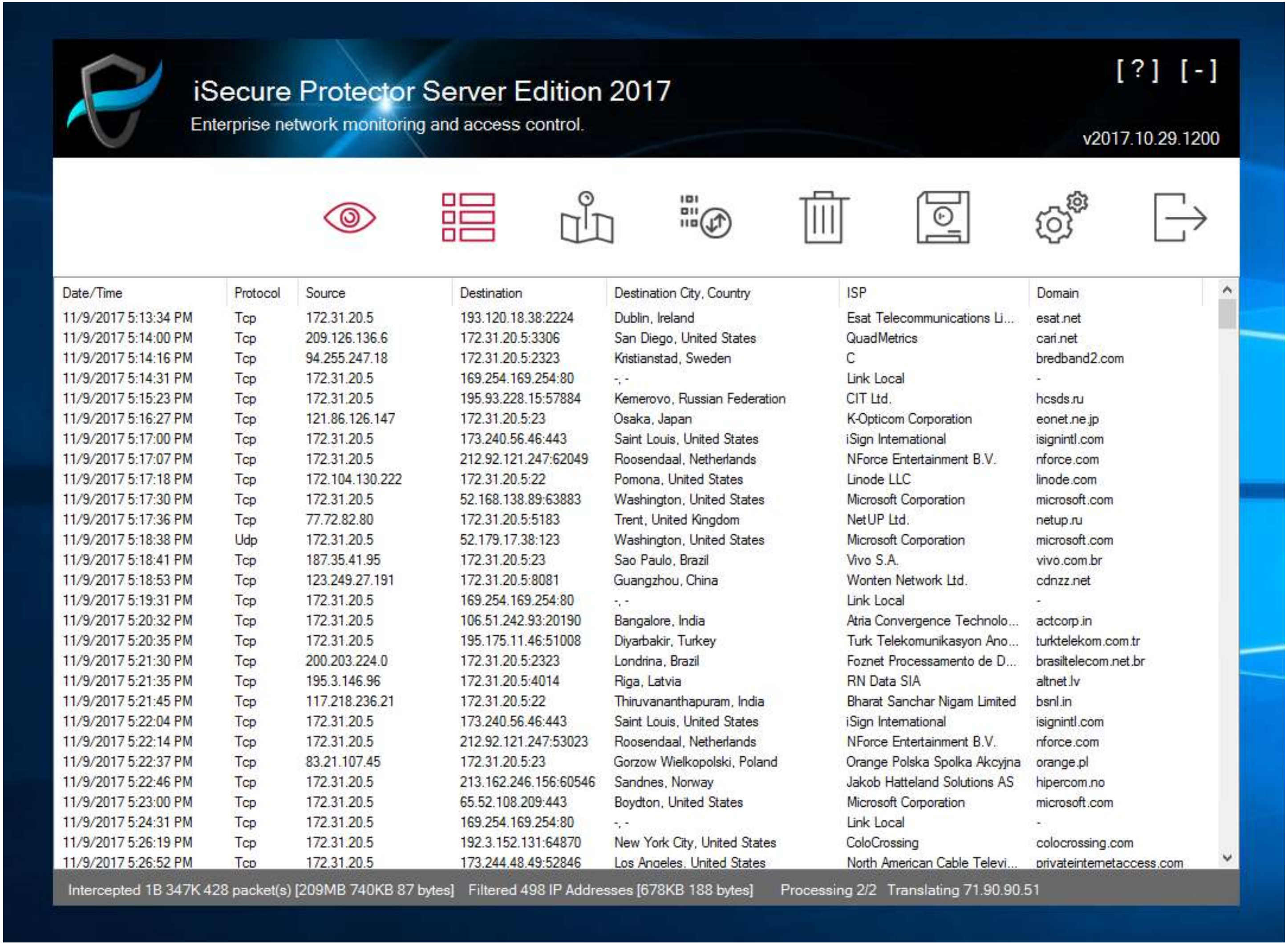
A request was sent to the iSign Team to install the iSecure Protector Server Edition on the Amazon AWS EC2 instance running Windows Server 2016. An iSign Team member was asked to create a user on the iSecure Protector Server Edition Management Portal and to enroll his/her biometric signature.

Requirements

1. Unrestricted access to server.
2. Smart Phone with on screen signing capability

Tests and Results

Chart 1 - iSecure Protector Server Edition Basic Monitoring End Result


iSecure Protector Server Edition 2017
Enterprise network monitoring and access control.
[?] [-]
v2017.10.29.1200

Date/Time	Protocol	Source	Destination	Destination City, Country	ISP	Domain
11/9/2017 5:13:34 PM	Tcp	172.31.20.5	193.120.18.38:2224	Dublin, Ireland	Esat Telecommunications Li...	esat.net
11/9/2017 5:14:00 PM	Tcp	209.126.136.6	172.31.20.5:3306	San Diego, United States	QuadMetrics	cari.net
11/9/2017 5:14:16 PM	Tcp	94.255.247.18	172.31.20.5:2323	Kristianstad, Sweden	C	bredband2.com
11/9/2017 5:14:31 PM	Tcp	172.31.20.5	169.254.169.254:80	-, -	Link Local	-
11/9/2017 5:15:23 PM	Tcp	172.31.20.5	195.93.228.15:57884	Kemerovo, Russian Federation	CIT Ltd.	hcsds.ru
11/9/2017 5:16:27 PM	Tcp	121.86.126.147	172.31.20.5:23	Osaka, Japan	K-Opticom Corporation	eonet.ne.jp
11/9/2017 5:17:00 PM	Tcp	172.31.20.5	173.240.56.46:443	Saint Louis, United States	iSign International	isignintl.com
11/9/2017 5:17:07 PM	Tcp	172.31.20.5	212.92.121.247:62049	Roosendaal, Netherlands	NForce Entertainment B.V.	nforce.com
11/9/2017 5:17:18 PM	Tcp	172.104.130.222	172.31.20.5:22	Pomona, United States	Linode LLC	linode.com
11/9/2017 5:17:30 PM	Tcp	172.31.20.5	52.168.138.89:63883	Washington, United States	Microsoft Corporation	microsoft.com
11/9/2017 5:17:36 PM	Tcp	77.72.82.80	172.31.20.5:5183	Trent, United Kingdom	NetUP Ltd.	netup.ru
11/9/2017 5:18:38 PM	Udp	172.31.20.5	52.179.17.38:123	Washington, United States	Microsoft Corporation	microsoft.com
11/9/2017 5:18:41 PM	Tcp	187.35.41.95	172.31.20.5:23	Sao Paulo, Brazil	Vivo S.A.	vivo.com.br
11/9/2017 5:18:53 PM	Tcp	123.249.27.191	172.31.20.5:8081	Guangzhou, China	Wonten Network Ltd.	cdnzz.net
11/9/2017 5:19:31 PM	Tcp	172.31.20.5	169.254.169.254:80	-, -	Link Local	-
11/9/2017 5:20:32 PM	Tcp	172.31.20.5	106.51.242.93:20190	Bangalore, India	Atria Convergence Technolo...	actcorp.in
11/9/2017 5:20:35 PM	Tcp	172.31.20.5	195.175.11.46:51008	Diyarbakir, Turkey	Turk Telekomunikasyon Ano...	turktelekom.com.tr
11/9/2017 5:21:30 PM	Tcp	200.203.224.0	172.31.20.5:2323	Londrina, Brazil	Foznet Processamento de D...	brasiltelecom.net.br
11/9/2017 5:21:35 PM	Tcp	195.3.146.96	172.31.20.5:4014	Riga, Latvia	RN Data SIA	altnet.lv
11/9/2017 5:21:45 PM	Tcp	117.218.236.21	172.31.20.5:22	Thiruvananthapuram, India	Bharat Sanchar Nigam Limited	bsnl.in
11/9/2017 5:22:04 PM	Tcp	172.31.20.5	173.240.56.46:443	Saint Louis, United States	iSign International	isignintl.com
11/9/2017 5:22:14 PM	Tcp	172.31.20.5	212.92.121.247:53023	Roosendaal, Netherlands	NForce Entertainment B.V.	nforce.com
11/9/2017 5:22:37 PM	Tcp	83.21.107.45	172.31.20.5:23	Gorzow Wielkopolski, Poland	Orange Polska Spolka Akcyjna	orange.pl
11/9/2017 5:22:46 PM	Tcp	172.31.20.5	213.162.246.156:60546	Sandnes, Norway	Jakob Hatteland Solutions AS	hipercom.no
11/9/2017 5:23:00 PM	Tcp	172.31.20.5	65.52.108.209:443	Boydton, United States	Microsoft Corporation	microsoft.com
11/9/2017 5:24:31 PM	Tcp	172.31.20.5	169.254.169.254:80	-, -	Link Local	-
11/9/2017 5:26:19 PM	Tcp	172.31.20.5	192.3.152.131:64870	New York City, United States	ColoCrossing	colocrossing.com
11/9/2017 5:26:52 PM	Tcp	172.31.20.5	173.244.48.49:52846	Los Angeles, United States	North American Cable Televi...	privateinternetaccess.com

Intercepted 1B 347K 428 packet(s) [209MB 740KB 87 bytes]   Filtered 498 IP Addresses [678KB 188 bytes]   Processing 2/2   Translating 71.90.90.51

According to the iSecure Protector Server Edition packet monitoring of both inbound and outbound activities, the **software detected 209 MB of data consumption from 11/6/2017 – 11/10/2017**. The reason for the high activities is due to the server being opened on all ports and there were many hacking attempts from various servers and computers throughout the Internet.

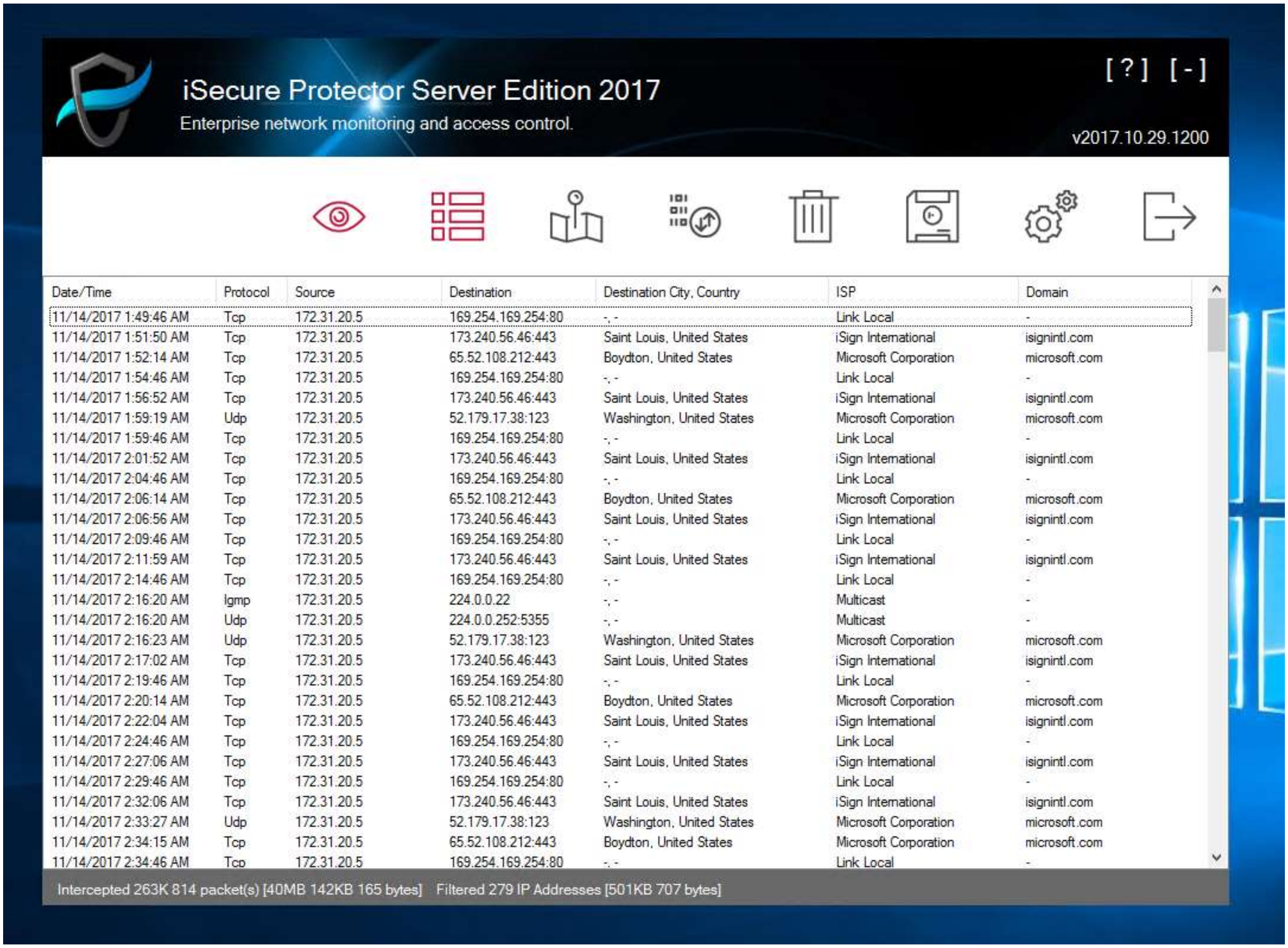
Connection to Server via RDP Test With iSecure Protector Server Edition on Basic Monitoring

Before we attempted to connect to the server, we asked the iSign Team to change the Administrator password and not disclose to anyone. Connect via RDP to attempt to use the default Administrator username: Administrator, and random password

Connections: 10   Password Attempts: 10   Success: 0

Without knowing the password and how complex it is, we were unable to break through. We were able to make the 10 connections to the server and see that it was running Windows Server 2016.

Chart 2 – iSecure Protector Server Edition Advance Monitoring End Result



iSecure Protector Server Edition 2017

Enterprise network monitoring and access control.

v2017.10.29.1200

Date/Time	Protocol	Source	Destination	Destination City, Country	ISP	Domain
11/14/2017 1:49:46 AM	Tcp	172.31.20.5	169.254.169.254:80	-, -	Link Local	-
11/14/2017 1:51:50 AM	Tcp	172.31.20.5	173.240.56.46:443	Saint Louis, United States	iSign International	isignintl.com
11/14/2017 1:52:14 AM	Tcp	172.31.20.5	65.52.108.212:443	Boydton, United States	Microsoft Corporation	microsoft.com
11/14/2017 1:54:46 AM	Tcp	172.31.20.5	169.254.169.254:80	-, -	Link Local	-
11/14/2017 1:56:52 AM	Tcp	172.31.20.5	173.240.56.46:443	Saint Louis, United States	iSign International	isignintl.com
11/14/2017 1:59:19 AM	Udp	172.31.20.5	52.179.17.38:123	Washington, United States	Microsoft Corporation	microsoft.com
11/14/2017 1:59:46 AM	Tcp	172.31.20.5	169.254.169.254:80	-, -	Link Local	-
11/14/2017 2:01:52 AM	Tcp	172.31.20.5	173.240.56.46:443	Saint Louis, United States	iSign International	isignintl.com
11/14/2017 2:04:46 AM	Tcp	172.31.20.5	169.254.169.254:80	-, -	Link Local	-
11/14/2017 2:06:14 AM	Tcp	172.31.20.5	65.52.108.212:443	Boydton, United States	Microsoft Corporation	microsoft.com
11/14/2017 2:06:56 AM	Tcp	172.31.20.5	173.240.56.46:443	Saint Louis, United States	iSign International	isignintl.com
11/14/2017 2:09:46 AM	Tcp	172.31.20.5	169.254.169.254:80	-, -	Link Local	-
11/14/2017 2:11:59 AM	Tcp	172.31.20.5	173.240.56.46:443	Saint Louis, United States	iSign International	isignintl.com
11/14/2017 2:14:46 AM	Tcp	172.31.20.5	169.254.169.254:80	-, -	Link Local	-
11/14/2017 2:16:20 AM	Igmp	172.31.20.5	224.0.0.22	-, -	Multicast	-
11/14/2017 2:16:20 AM	Udp	172.31.20.5	224.0.0.252:5355	-, -	Multicast	-
11/14/2017 2:16:23 AM	Udp	172.31.20.5	52.179.17.38:123	Washington, United States	Microsoft Corporation	microsoft.com
11/14/2017 2:17:02 AM	Tcp	172.31.20.5	173.240.56.46:443	Saint Louis, United States	iSign International	isignintl.com
11/14/2017 2:19:46 AM	Tcp	172.31.20.5	169.254.169.254:80	-, -	Link Local	-
11/14/2017 2:20:14 AM	Tcp	172.31.20.5	65.52.108.212:443	Boydton, United States	Microsoft Corporation	microsoft.com
11/14/2017 2:22:04 AM	Tcp	172.31.20.5	173.240.56.46:443	Saint Louis, United States	iSign International	isignintl.com
11/14/2017 2:24:46 AM	Tcp	172.31.20.5	169.254.169.254:80	-, -	Link Local	-
11/14/2017 2:27:06 AM	Tcp	172.31.20.5	173.240.56.46:443	Saint Louis, United States	iSign International	isignintl.com
11/14/2017 2:29:46 AM	Tcp	172.31.20.5	169.254.169.254:80	-, -	Link Local	-
11/14/2017 2:32:06 AM	Tcp	172.31.20.5	173.240.56.46:443	Saint Louis, United States	iSign International	isignintl.com
11/14/2017 2:33:27 AM	Udp	172.31.20.5	52.179.17.38:123	Washington, United States	Microsoft Corporation	microsoft.com
11/14/2017 2:34:15 AM	Tcp	172.31.20.5	65.52.108.212:443	Boydton, United States	Microsoft Corporation	microsoft.com
11/14/2017 2:34:46 AM	Tcp	172.31.20.5	169.254.169.254:80	-, -	Link Local	-

Intercepted 263K 814 packet(s) [40MB 142KB 165 bytes] Filtered 279 IP Addresses [501KB 707 bytes]

iSecure Protector Server Edition was configured to close all ports from 1-65535 and only allow specific to be open when needed. As the result of selected port opening, iSecure Protector Server Edition detected 40 MB of data consumption from 11/10/2017 – 11/14/2017.

Connection to server via RDP Test with iSecure Protector Server Edition in Protection Mode

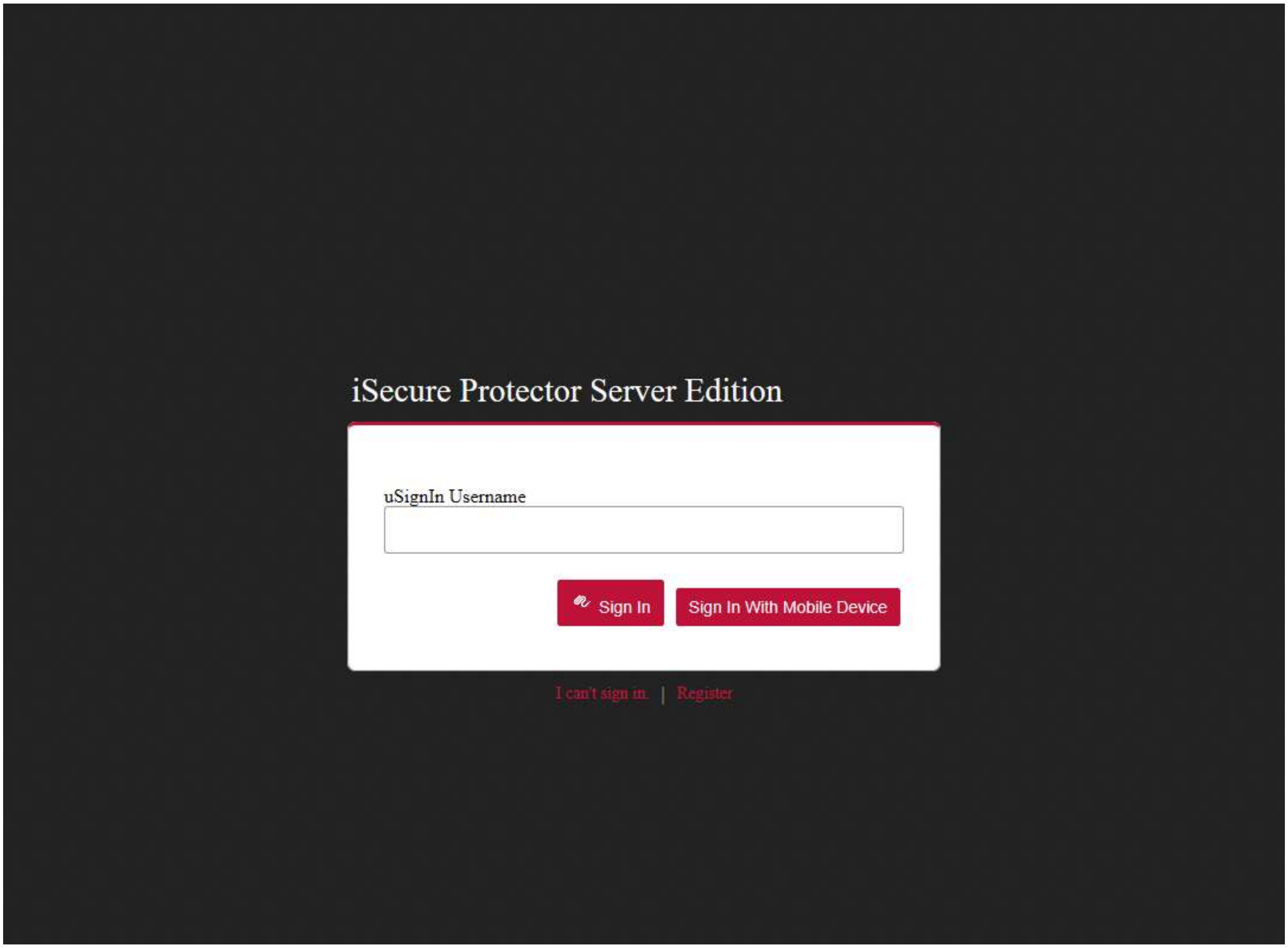
We asked the iSign Team for the username and password to connect to the Amazon AWS EC2 server. Using the username Administrator and the password set for the Administrator as crX.4@=W*eaRdlcv$lWj?ieLqlF)YJ7i.

Connections: 0   Password Attempts: 0   Success: 0

Because iSecure Protector Server Edition closed all ports and only allow it to open to specific IP Addresses, we were unable to connect to the server to make any attempts at hacking the server.

Turning on RDP Port 3389 to allow connections to the server

A request was sent to the iSign Team to open the RDP Port 3389 and to one of their IP Addresses. We also requested the iSign Team to give us the uSignIn Username (isecureprotector). Once that has been accomplished, we proceeded to https://www.isignapps.com/iSecureProtector2017/SE and use the isecureprotector username to log into the system.


iSecure Protector Server Edition
uSignIn Username
Sign In
Sign In With Mobile Device
I can't sign in. | Register

Using the provided uSignIn Username, we began to attempt to break in.

1. Enter the uSignIn Username
2. We attempted to sign using a touchscreen laptop, guessing the signatures

Signature Sign In
Attempts: 2 Failed: 2 Success: 0

After 2 failed attempts using a signature that we believed to be the signature of the uSignIn username isecureprotector, our IP Addressed was blocked. We contacted the iSign Team to unblock the IP Address so that we can make connections to the server.

Signature Sign In with Mobile Device
Attempts: 2 Failed: 2 Success: 0

Upon signing in with mobile device, we were unable to sign in because isecureprotector uSignIn username was already registered to another device, which we did not have possession at the time; simulating a real world situation.

Sign In with Password
Attempts: 10 Failed: 10 Success: 0
We used the Can’t Sign In feature to attempt to get the passcode to log into the account and were unsuccessful because the passcode was sent to the mobile phone that was registered to the account. We did not have possession of the mobile phone that was associated to the isecureprotector username.

Conclusion
After thorough testing and data collections, I have concluded that the iSecure Protector Server Edition reduced the bandwidth consumption from 209MB to 40MB, which is a 500% bandwidth reduction. The iSecure Protector Server Edition was 100% effective in blocking unknown sources from remote desktop. Even with selective IP Address and selective port opening of 3389, the iSecure Protector Server Edition blocked all unauthorized IP Addresses.

The iSecure Protector Server Edition management portal with biometric signature and 5-Factor authentication was 100% effective in identifying unknown sources and black listed the IP Addresses immediately. Because we could not obviously reproduce the biometric signature of the isecureprotector user, the system immediately blocked our IP Addresses after 2 failed attempts.

Trying to break in using the passcode option with a mobile device was also unsuccessful since our mobile phone was not recognized.

iSecure Protector Server Edition is certainly a great tool for both reducing bandwidth and blocking all hacking attempts.

Assistant Research Professor, Arizona State university
Title

Ziny Zho

Ziming Zhao

2017/11/24
Date