Internet 2.0
RELENTLESS SECURITY

DURHAM COLLEGE TECHNICAL ANALYSIS OF INTERNET 2.0's NEXT GENERATION CLOAKING FIREWALL

EXECUTIVE SUMMARY

The following document provides an overview and technical analysis of cyber security-based appliance company Internet 2.0 from the Durham College Centre for Cybersecurity Innovation. With the growth of internet generation and virtual environment, securing, protecting, and monitoring of the network is a must.

Internet 2.0 is a new secure version of accessing the internet. To balance both privacy and security, it uses an advanced encryption technology and next generation cybersecurity appliance with an easy to interact software.

The following document includes the product overview and the security technology developed by Internet 2.0, as well as market comparison with competitors.

The team at Durham College has studied the application from a technical and operational perspective. Keeping in mind the growing need for affordable cybersecurity endpoint management solutions, Durham College students in cybersecurity have created a test environment and reported on their initial findings. These findings can guide future opportunities for collaboration with and growth of Internet 2.0.

HOW IT WORKS?

As we know a firewall is a piece of hardware or software that helps prevent malware and a malicious attack from entering a computer or network through internet. Internet 2.0's product 'IP-100', is an Advanced Hardware firewall which are systems that are independent of the computer or network they protect that filters the internet as information passes through them into the computer or network.

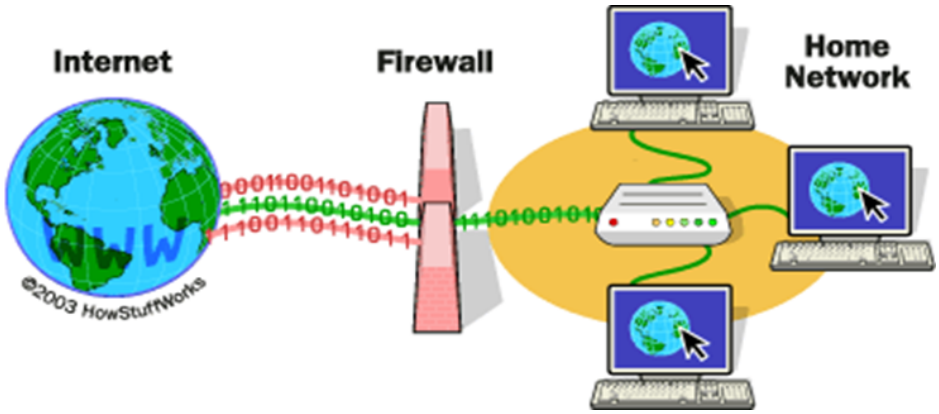
In general, a hardware firewall works by examining the data that flows in from the internet and verifying whether that information is safe. Simple firewalls are basically packet filters that examine the data itself for information such as its location and source.

IP-100 is a combination of a next generation hardware firewall combined with secure gateway, which can be connected with the router/switch to secure a network or individual computer.

These types of firewalls have their benefits for homes and small businesses because they require little to no setup, and multiple endpoints (computers) can be protected and monitored from one piece of equipment.

As you can see in Figure 1 below, this kind of hardware firewall can be used in conjunction with the internet to filter the network from malicious programmes and can be used in conjunction with individual nodes or endpoints (i.e. computer). This is done to ensure that performance doesn't suffer as a result of the computer using resources in the background to filter, secure and monitor the network.

Figure 1: How a hardware firewall works.



ADVANTAGES AND DISADVANTAGES

Advantages

IP-100 firewall is one of the best protections ever made against internet threats. It prevents your computer from cyber-attacks and various other threats on the internet.

1. Intrusion Detection and Monitoring

One of the major responsibilities of a firewall is to monitor the traffic passing through it in the form of packets. It inspects each of the packets for any hazardous threat based on the policies enforced and reports, flags or blocks them immediately. Intrusion detection with its one-stop dashboard makes it easy to implement policies and monitor traffic. It is just like the SIEM system.

2. Obfuscation

One of the most essential features of Internet 2.0. Making it an industry standard, this technology paired with the monitoring dashboard makes it an easy-to-use security appliance to fit the needs of modern era security requirements from malware protection to trojan detection. It makes it difficult for hackers to scan and flag the network.

3. Advanced Encryption

Hackers on the internet constantly look to manipulate and break into the system for their illegal and malicious intent. Activities can include spreading viruses or getting information to do industrial espionage or selling information for money. Advance encryption secures the network and comes in handy in user authentication to limit and control access throughout the network.

4. Access Control

With Internet 2.0, access policy can be implemented for certain hosts and services. Some hosts can be exploited by attackers. An organisation can configure and customise their company policy to ensure security and reduce the chances of breaches if any.

5. Better Privacy

One of the major concerns of the modern-day information technology company is hackers and people with malicious intent that are constantly looking for clues and information to abuse the system or break into the system. However, using a firewall such as Internet 2.0 offers a wide variety of services that can help better monitor and administer and protect information and data.

6. Performance

IP-100, being a hardware firewall does not depend on the computer system resources like software firewalls do, which in turn limits the system overall performance such as the processing power and RAM resources.

7. General advantages

Other general advantages include speed, advanced encryption, the one-stop dashboard to manage, and no interference to the network.

Disadvantages

1. Cost

Though it is an investment towards securing the business operation of the company, in addition to buying the hardware such a firewall requires installation and maintenance which is very costly in the market. This causes a challenge for IP-100 to become an instant success in the market which is so competitive and expensive.

2. User Restrictions

Security comes with a cost restriction, as it is easier to monitor and protect a specific set of networks or ports and web pages etc. While average users have no problem, this can be an issue for large organisations. The policies used by the firewall can be strict enough to prevent employees from performing operations, thereby impacting the overall productivity. Employees may also be prompted to use the backdoor exploits. However, this can lead to security problems since the data travelled through these exploits are not examined properly.

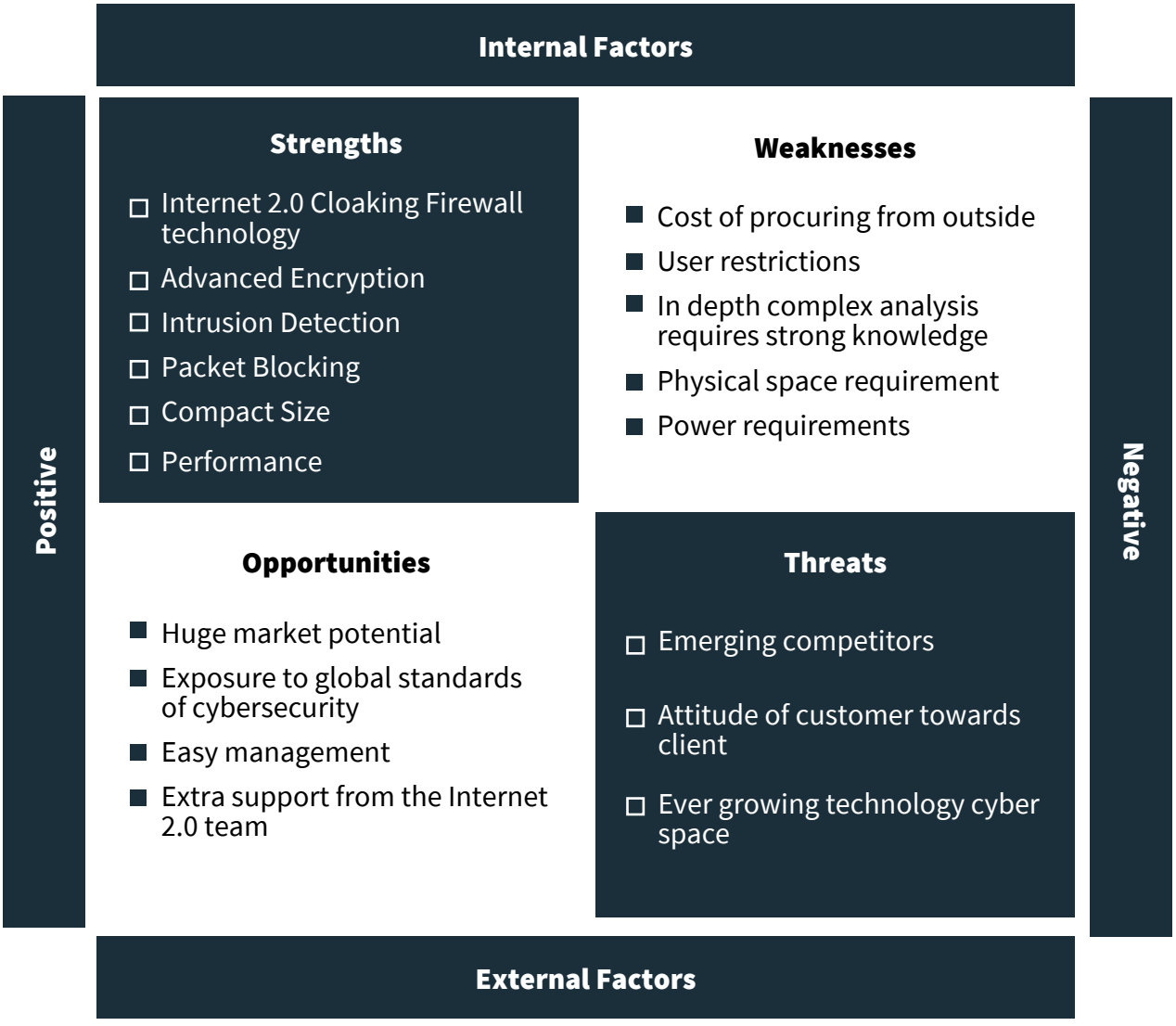
3. Malware Attacks

Even though firewalls can block most trojan and known threats, they prove to be defenceless against other types of malware. Malware can enter the network or system in the form of trusted data even with the advanced encryption running in the background. Accordingly, it is still recommended strongly to also have a good anti-malware software, as that is the only way to flag and remove them.[1]

4. Complex Operations

Even though for small businesses the firewall maintenance is made easy, it is not the case for large organisations, large organisations require a set of staff for operating them to maintain a secure and safe environment.

SWOT ANALYSIS



1 Note all IDS/IPS devices using signature correlation do not detect malware if the traffic passing through the device is encrypted. This is a major problem with using only IDS/IPS.

COMPETITORS

The below table shows that major competitors in the market are Fortinet, CISCO, Palo Alto, Sonic Wall and PF Sense.

Product	Firewall Throughput	Max New Session Per Second	Max Concurrent Sessions	Integrated I/O	Serial Ports	Form Factor
Fortinet: FortiGate 80 E	460 Mbps	3000	1.3 million	12x Gigabit	LAN	Desktop
CISCO: Cisco ASA-5508	450 Mbps	1000	100000	8x Gigabit Ethernet	LAN and USB	Rackmount
SonicWall: SonicWall SOHO 250	600Mbps	3000	50000	3x Gigabit Ethernet	LAN and USB	Desktop
PF sense: PF sense SG-1100	500 Mbps	N/A	1 million	3x Gigabit Ethernet	LAN and USB	Desktop
Internet 2.0: IP-100	600 Mbps	N/A	N/A	12x Gigabit Ethernet	LAN and USB	Desktop
Firewalla: Firewalla Gold	400 Mbps	N/A	40,000	3x Gigabit Ethernet	LAN	Desktop

RECOMMENDATIONS

Major things to consider when choosing a hardware firewall are the following:

Firewall Throughput

This applies to hardware firewalls and these applications have a varied range of operation and range of firewall throughput to offer. It also depends on the number of network users which will define the throughput.

Devices Monitoring

The unique thing about Internet 2.0 is the product dashboards. The advanced firewall should be capable of finding a device by username and not only just by IP to better navigate and monitor the network.

Protection and Threat Prevention

Internet 2.0 can track and control all the applications and information on the network, limit traffic, reduce risk to the network by only allowing applications to be used in a monitored environment thereby enabling the scanning from within the network for threat prevention.

Obfuscation

Internet 2.0 is revolving around this information technological tool of Obfuscation which gives it the edge over the other hardware firewall in the magnet.

Remote User Coverage

Advanced firewalls should be able to monitor and control traffic coming in and going out among the remote users who are connected to your infrastructure.

Streamlined Security Infrastructure

Advanced firewall installed like building antivirus protection, spam filtering, and deep packet inspection and filtering.

Access Control

With the easy-to-use dashboard and various firewall configurations that can be applied to the network users, organizations could prohibit access to applications, etc.

Price

Price is always a factor, but when it comes to choosing the right firewall, it is important to think about the business scalability and budgeting to envision future growth and security of the company data.

Manufacturing

Manufacturing of such business facility will increase the industrial exposure and the contribution to the world of Information security.

Customer Service and professional Team

The team of Internet 2.0 is diverse and diligent professional, with a variety of experience to better cater to the needs of individual and business.

APPLICATION IN DURHAM REGION

Extra Support

Hardware firewall products commonly provide support for assistance with the configuration, troubleshooting and the ability to make expeditious adjustments which will help hardening and security of personal information of residents and business in Durham regions once they become clients of Internet 2.0.

Managing traffic and control over ports for better security and monitoring

A set of default guidelines can be installed that apply to entire traffic that flows through out the firewall. This technology can deploy in local hospitals, schools, universities, colleges, trains system, mobile networks etc.

For example, phishing attacks and trojans are common in all businesses. Hackers are always on a look out to break into the network. Humans are the biggest threat to the network because of their lack in compliance towards rules. Consider a school environment, where students are curious and visit different webpages. This needs to be monitored as a lot of personal information are stored in server archives in an era where information is power. Open port and backdoor can be abused by tricking gullible children or human by just a click. To protect against this Internet 2.0, is an ideal solution. Same can be said for hospital, small business etc.

VERDICT

Internet 2.0 comes loaded with all the modern features needed to better secure the network device with its 'Obfuscation' technology, the process of hiding the original data with modified content such as characters or other data. The process is used to safeguard information classified as personally identifiable information etc.

It comes with an interactive dashboard, advanced encryption, intrusion detection, advanced firewall, configurable routing, packet blocking and many more features. In terms of growth, the company has a unique technology that makes it special and attractive to niche markets. Also, the cost of manufacturing will boost the economy and would be good exposure and huge contribution to the community of cybersecurity. We strongly recommend this for individuals and small to medium businesses.

WHO IS THE DURHAM COLLEGE CENTRE FOR CYBERSECURITY INNOVATION?

Durham College Centre for Cybersecurity Innovation, an initiative of Durham College supports the community with the increased demand for security professionals. Durham college already has a Graduate Certificate program with provides industry level training from different cybersecurity professionals who help nurture students with Computer Networking and Programming knowledge, how they can be successful in the community with their knowledge, and latest trends to defend our nation against the rise of cybercrime in the virtual workspace.

The Centre for Cybersecurity Innovation provides aspiring cybersecurity professionals a leading-edge in cybersecurity to prepare for the ever changing and complex threat landscape, and a blend of technical and soft skills to better understand the industry and make them more industry ready. Thanks to the prestigious reputation of Durham College within the community, public and private sector organisations have allowed our students to work on different projects granting them the key experience needed for success.

We have been involved with Internet 2.0 for close to a year now. We are thankful for the faith they have showed in us and our students, allowing us to work with them on their flagship devices. Recently, a team of promising graduates from our cybersecurity and artificial intelligence programme have worked on broad research on the Next Generation Hardware Firewall. Our diligent team have been working on building scenarios to test the efficiency of the products, including a sandbox environment network which was prepared to test the products. Further, a framework has also been identified to report our finding to the organisation to help them better their research, and provides us a learning opportunity about the global market.

Internet 2.0

RELENTLESS SECURITY

AUSTRALIA

L1, 18 National Circuit, Barton ACT, 2600

ABN: 17 632 726 946

UNITED STATES

Suite 100, 211 N Union St Alexandria, 22314

EIN: 86-1567068

AUS: 1300 583 007
INTL: +611300583007
contact@internet2-0.com

DURHAM COLLEGE
SUCCESS MATTERS

CENTRE FOR CYBERSECURITY INNOVAT10N

OSHAWA CAMPUS
2000 Simcoe St. N.
Oshawa, ON, Canada L1G 0C5

T: 905 721 3223

CentreForCybersecurityInnovation@durhamcollege.ca