NET Institute*

www.NETinst.org

Working Paper #07-19

September 2007

Assessing the Value of Network Security Technologies

Huseyin Cavusoglu
University of Texas at Dallas

Hasan Cavusoglu
University of British Columbia

* The Networks, Electronic Commerce, and Telecommunications ("NET") Institute, http://www.NETinst.org, is a non-profit institution devoted to research on network industries, electronic commerce, telecommunications, the Internet, "virtual networks" comprised of computers that share the same technical standard or operating system, and on network issues in general.

ASSESSING THE VALUE OF NETWORK SECURITY TECHNOLOGIES: THE IMPACT OF CONFIGURATION AND INTERACTION ON VALUE[1]

Huseyin Cavusoglu
School of Management
The University of Texas at Dallas
Richardson, TX 75083
huseyin@utdallas.edu

Hasan Cavusoglu
Sauder School of Business
University of British Columbia
Vancouver, BC V6T1Z2
cavusoglu@sauder.ubc.ca

Abstract

Proper configuration of security technologies is critical to balance the access and protection requirements of information. The common practice of using a layered security architecture that has multiple technologies amplifies the need for proper configuration because the configuration decision about one security technology has ramifications for the configuration decisions about others. We study the impact of configuration on the value obtained from a firewall and an Intrusion Detection System (IDS). We also study how a firewall and an IDS interact with each other in terms of value contribution. We show that the firm may be worse off when it deploys a technology if the technology (either the firewall or the IDS) is improperly configured. A more serious consequence for the firm is that even if each of these (improperly configured) technologies offers a positive value when deployed alone, deploying both may be detrimental to the firm. Configuring the IDS and the firewall optimally eliminates the conflict between them, resulting in a non-negative value to the firm. When optimally configured, we find that these technologies may complement or substitute each other. Further, we find that while the optimal configuration of an IDS is the same whether it is deployed alone or together with a firewall, the optimal configuration of a firewall has a lower detection rate (i.e., allow more access) when it is deployed with an IDS than when deployed alone. Our results highlight the complex interactions between firewall and IDS technologies when they are used together in a security architecture, and, hence, the need for proper configuration in order to benefit from these technologies.

Keywords: Information Security, Software Configuration, Analytical Modeling
JEL Numbers: C72, D81, L20, L86

[1] We thank the NET Institute www.NETinst.org for financial support.

1. Introduction

Software configuration refers to the process of setting software quality parameters to meet specific user requirements. Proper configuration is particularly critical for information technology (IT) security software as evidenced by frequent warnings by security experts about risks from using default ("out-of-the-box") settings (McCarthy 1998). The commonly cited risk is that default configurations are insecure and using them allows hackers to exploit known software vulnerabilities more easily (Piessens 2002). Configuration is also important from an operational economics perspective. For instance, CERT's guidelines (CERT 2001) for installing security software recommend that firms adjust configuration to balance their own security and operational requirements[2]. Further, configuration becomes more important in an IT security context because firms typically deploy a layered security architecture that has diverse security software.

The primary goal of IT security is balancing the conflicting needs of information protection and information access. To achieve this goal, firms typically deploy technologies such as firewalls and intrusion detection systems (IDSs), along with physical security measures such as manual investigations and physical access controls. The deployment of multiple technologies makes configuration challenging because the configuration decision regarding one technology has ramifications on the configuration decisions of others, and, consequently, configuration decisions will have to be coordinated to achieve optimal overall performance. A recent Gartner report highlights the problem associated with excessive false alarms generated by IDSs that are not configured properly (Gartner 2003). Further, the debate within the IT security community about whether a firewall obviates or complements the need for IDS and vice versa (Magalhaes 2004, Gigabit 2004) illustrates the mixed experiences about the performance of these technologies when deployed together. Axelsson (2000) summarized the debate as "The best effort [security] is often achieved when several security measures are brought to bear together. How should intrusion detection collaborate with other security mechanisms to this synergy effect? How do we ensure that the combination of security measures provides at least the same level of security as each applied singly would provide, or that the combination does in fact lower the overall security of the protected system?", and he continued "…they [these questions] remain largely un-addressed by the research community. This is perhaps not surprising, since

[2] Similar observations have been made for explosives detection systems used by airports (NMAB 1998).

many of these questions are difficult to formulate and answer." The research described in this paper seeks to shed light on the above questions raised by the security community regarding the configuration of and interaction between security technologies. Specifically, we study (i) how a firm should configure a firewall and an IDS when they are deployed together or separately in the security architecture of the firm, (ii) how the firewall and the IDS interact with each other in value creation (i.e., whether they are complementary, substitutes or conflicting), and (iii) how optimal configuration impacts the type of interaction between these security technologies.

The most significant findings of this study are the following. We show that the firm may be worse off when it deploys a technology (either the firewall or the IDS) if the technology is improperly configured. A more serious consequence for the firm is that even if each of these (improperly configured) technologies offers a positive value when deployed alone, the firm may realize a lower value when it deploys both than when it deploys only one of them. Configuring both the IDS and the firewall optimally eliminates the conflict, and hence, the detrimental effect of deploying them together. When optimally configured, a firewall may complement (i.e., enhances the value of) an IDS and vice versa provided it is optimal for the firm to prohibit external access in the absence of a firewall. We find that an optimally configured IDS behaves as a deterrent, and, hence, allowing external access may become attractive to the firm when it deploys the IDS whereas the preventing external access may be more desirable when it does not deploy the IDS. While the optimal configuration of an IDS remains the same whether or not a firewall is deployed, a firewall should be configured to operate at a lower detection rate (i.e., allow more access) when it is used with an IDS than without.

The remainder of the article is organized as follows. We review the relevant literature in Section 2. We discuss the configuration problem and our model in section 3. We derive the equilibrium hacking and investigation strategies in section 4. In section 5, we analyze the value of firewall and IDS when they are deployed at their default configurations, and in section 6, we analyze optimal configuration decisions. In Section 7, we show the robustness of our results by analyzing alternative model specifications. In section 8, we discuss the implications of our results and future research directions.

2. Related Literature

Research on information security technologies has analyzed both the technical and the economic aspects surrounding the design and implementation of security controls. The technical research

has focused largely on the design of algorithms related to firewalls, IDSs and others such as encryption. Various approaches to firewall design are discussed in (Holden 2004, Gouda and Liu 2004). IDS design uses two broad approaches. The significant developments in signature-based IDSs are highlighted in (Garvey and Lunt 1991, Porras and Kemmerer 1992, Ilgun 1992, Lunt 1993, Kumar and Spafford 1996, Monrose and Rubin 1997). The algorithms employed in anomaly-based IDSs are presented in (Lunt and Jagannathan 1988, Lunt 1990, Lunt 1993, D'haeseleer et al. 1996, Porras and Neumann 1997, Frincke et al. 1996, Neumann and Porras 1999, Zamboni and Spafford 1999). Since the environments where firewalls and IDSs are deployed vary, these technologies are designed so that their behavior can be tuned by individual firms through the process of configuration to fit their operating environments. We focus on configuration issues faced by firms that deploy these technologies and consequently, we assume that their design is exogenous to our problem.

Research on the economics of security technologies is based on the notion that security technologies are imperfect, and, therefore, policies based on the cost-benefit tradeoff are required to support these technology implementations. The imperfections of security technologies are typically captured using false positive and false negative error rates. Since different firms may have different tolerance levels for false positives and different acceptable levels for detection rate, researchers have begun to investigate how to configure a given IDS to fit a specific deployment environment. Cavusoglu, Mishra, Raghunathan (2005) analyze the value of IDSs and show that IDSs offer a positive value only when they deter hackers. Ulvila and Gaffney (2004) propose a decision analysis approach to configure IDSs. Cavusoglu and Raghunathan (2004) compare decision analysis and game theoretic approaches to configure IDSs and show that the game theoretic approach is superior to the decision analysis approach. Cavusoglu, Ogut, and Raghunathan (2006) analyze optimal waiting time policies to deal with the problem of false alarms in an IDS. Researchers also investigated the issue of configuration of firewalls. Yue and Baghci (2003) consider how to tune the quality parameters of a firewall to maximize its benefit. All these studies in this stream of research focus on a single technology. None of them considers the issue of configuration when multiple technologies are deployed as part of a layered security architecture and, therefore, does not address interaction between security technologies.

Researchers have also addressed other aspects of information security such as security vulnerability discovery and disclosure (Schechter 2002, Ozment 2004, Cavusoglu et al. 2007,

Nizovtsev and Thursby 2005), security information sharing (Gordon et al. 2003, Gal-Or and Ghose 2005), patch management (Cavusoglu et al. 2008, August and Tunca 2005), and security investments and risk management (Ogut et al. 2005). However, this stream of research does not model specific security technologies, and, therefore do not provide insights into how security technologies should be configured to minimize the cost of security.

3. Model Description

We model an environment in which a firm is evaluating the adoption of security technologies to extend its enterprise by providing access to outside vendors and partners. The common practice in such contexts is to implement a 'defense-in-depth' IT security architecture (Whitman and Mattord 2003). In this architecture, three layers – the firewall at the network (periphery) layer, the IDS at the host (middle) layer, and manual investigation at the data (interior) level – are employed to provide security. Firewalls are implemented to control the traffic between a trusted network ("Internal") and un-trusted ("External") networks. The internal network is trusted because the firm can exercise its own security policies over the network. The firm does not have such control over external networks. Even though external networks are un-trusted, the firm may still want to allow communication from external networks. In this setup a firewall controls the traffic between internal and external networks using an Access Control List (ACL). An IDS monitors events occurring in host and internal systems and warn human experts about suspected intrusions. A key difference between firewall and IDS technologies is that while a firewall takes actions against a suspected intrusion by blocking the traffic, an IDS only sends an alarm to the security administrator about a potential intrusion, who may terminate the user's session[3]. Another difference is although an IDS can detect intrusions originating from both internal and external networks, a firewall can prevent intrusions coming from only external networks.

Both a firewall and an IDS are configurable within their design profiles. The design profile of a firewall or an IDS is depicted as a curve, known as the ROC curve, that relates the probability of true detection (stopping an illegal external user in case of a firewall, and raising an alarm for an unauthorized activity of a user in case of an IDS) and the probability of false detection (stopping a legal external user in case of firewall, and raising an alarm for a normal activity of a user in case of IDS). The shape of the ROC curve depends on the algorithm used by

[3] There are also active response IDSs that take action against suspected intrusions on their own. Due to high false positives, many commercial IDSs do not support active response. Therefore we assume that the firm uses a passive IDS in its security architecture in this paper.

the technology. In a typical ROC curve, the probability of true detection is higher than the probability of false detection, and the probability of true detection is an increasing concave function of the probability of false detection (Trees 2001). We discuss the derivation of an ROC curve in Section 3.2. Security administrators can configure an IDS or a firewall to operate at a specific point on the ROC curve by tuning certain parameters in the case of an IDS or by modifying the ACL (rules and its attributes) in a firewall.

3.1 The Model

We discuss the three broad components of our model- user, firm, and technology- in the following paragraphs.

User: We consider two types of users. All internal users have access to the system from inside the firewall, i.e., they do not go through the firewall. The external users access the system from outside the firewall, and, hence, they are validated by the firewall, if one exists, before accessing the system. We assume that ε fraction of users is external users. We classify users also into legal and illegal users. Legal users are those that offer a positive payoff to the firm if they do not abuse their privileges whereas illegal users do not offer a positive payoff the firm under any circumstances. While all internal users are legal users of the system, only a proportion ζ of external users are legal users. The reason for this difference between internal and external users is that, as explained previously, the firm can control its internal users by deploying its own authentication and other access control mechanisms, but the firm does not have a similar control over external users[4]. Clearly, an ideal firewall will allow all legal external users and stop all illegal external users. After gaining access to the system, a user (internal or external) may choose to abuse (intrude) the system by executing unauthorized actions. The objective of an IDS is to detect intrusions by internal as well as external users.

A user (internal or external) that abuses the system, whom we refer to as a hacker, derives a benefit of μ, if the intrusion is undetected. If the intrusion is detected, the hacker incurs a penalty of β for a net benefit of $(\mu-\beta)$. We assume that $\mu \leq \beta$; that is, a hacker that is detected does not enjoy a positive benefit. Users that gain access to the system choose to hack depending on factors such as μ, β, and the likelihood that they will get caught. We denote the probability of

[4] Although all internal users are assumed to be legal users, they can still misuse their privileges, and our model captures this aspect. Our model can also be easily extended to the case where a proportion of internal users is assumed to be illegal. The results do not change qualitatively.

hacking for a user as ψ. An illegal external user could also derive an additional utility solely from cracking the firewall; that is, even if the illegal external user does not abuse the system after gaining access, he/she may enjoy some utility. Because this additional utility does not change our results, we have normalized it to zero.

Firm: We consider a single firm, which may deploy only a firewall, only an IDS, both a firewall and an IDS, or neither in its security architecture. The payoffs to the firm under different scenarios of system usage are given in Table 1.

Table 1. The Payoffs to the Firm

	Normal Use	Undetected Intrusion	Detected Intrusion
Internal User	ω	$-d$	$-(1-\phi)d$
Legal External User	ω	$-d$	$-(1-\phi)d$
Illegal External User	0	$-d$	$-(1-\phi)d$

We normalize the payoff to the firm from an external illegal user that has gained access but does not further abuse the system to zero. We assume that the benefit to the firm under normal use by a legal user is ω. When a user hacks the system and the hacking is undetected, the firm incurs a damage of d. However, the firm can detect hacking by manually investigating user log files. Firms can confirm or rule out hacking only through manual investigation. In general, manual investigation is too costly to be done all the time. When the firm does not deploy an IDS, the firm may manually investigate a proportion of users. When the firm deploys an IDS, the firm may investigate a proportion of users that generate alarms from the IDS and a possibly different proportion of users that do not generate alarms. The firm incurs a cost of c each time it performs a manual investigation. We assume that manual investigations confirm or rule out intrusions with certainty.[5] If the firm detects hacking, the firm prevents or recovers a fraction, $\phi \leq 1$, of d. It is reasonable to assume that $c \leq \phi d$ so that the firm's cost of investigation is not higher than the benefit it gets if it detects an intrusion. The firm's payoff parameters may not be independent, but dependence among these parameters does not change the essential results of the paper.

Firewall: We measure the effectiveness of a firewall through two parameters: P_D^F and P_F^F. P_D^F is the probability that the firewall stops an illegal external user. P_F^F is the probability that the

[5] Our results do not change qualitatively when manual investigation is imperfect.

firewall stops a legal external user. In practice, the value of P_F^F is likely to be low, and P_D^F is likely to be high. However, for a given firewall, these parameters are not independent. Security stance of the firm, reflected by its configuration decision, determines the combination of P_D^F and P_F^F for the firewall deployed. While the paranoid approach in configuration leads to a high P_D^F and P_F^F , the open approach results in a low P_D^F and P_F^F. For a given firewall, we capture the relationship between P_D^F and P_F^F as $P_D^F = \left(P_F^F\right)^{r_F}$. We derive this functional form for the ROC curve in Section 3.2.

IDS: The model for the IDS is similar to that of a firewall. That is, P_D^I is the probability that the IDS raises an alarm for an intrusion. P_F^I is the probability that the IDS raises an alarm when there is no intrusion. These quality parameters are determined by the configuration for a given technology profile of the IDS. As in the case of firewall, the probability of detection and the probability of false alarm are related by $P_D^I = \left(P_F^I\right)^{r_I}$, where r_I captures the technology profile of the IDS.

3.2 Derivation of ROC Curve

The ROC curve for a security technology can be derived analytically or experimentally (Durst et al. 1999, Lippmann et al. 2000). In the following paragraph, we illustrate the analytical derivation of the ROC curve for a firewall. Similar approach is also used to derive the ROC curve for an IDS, and is discussed in Cavusoglu, Mishra, and Raghunathan (2005). Consider a firm that is configuring the ACL for a firewall. Firms decide whether to put an external site (say an IP address) in the 'deny' list or 'permit' list of a firewall based on the level of threat ("threat index") associated with the traffic coming from that site. The threat index represents the estimated probability that a user from that site is an illegal user. A firm includes a site in the 'permit' list only when the threat index for that site is below a threshold value. For instance, Cisco PIX firewall relies on this type of index values to deny or permit traffic. Similarly, IDSs classify a user as hacker or not based on whether a numerical score computed from the transaction history (i.e., anomaly index) exceeds a threshold value.

Let the estimated threat index for a site be x, and the threshold value that determines whether to put the site in the 'permit' or in the 'deny' list be t. Let a site for which $x > t$ be put in the 'deny' list. We assume that $f_T(x)$ and $f_U(x)$ are the probability density functions of x for

"trusted" sites and "untrusted" sites, respectively. We assume that $f_U(x)$ stochastically dominates $f_T(x)$, i.e., $F_T(x) \geq F_U(x), \forall x$. This assumption implies that trusted sites are less of a threat than untrusted sites. It follows that

$$P_D^F = \int_t^\infty f_U(x)dx \text{ and } P_F^F = \int_t^\infty f_T(x)dx$$

We can easily show that $P_D^F > P_F^F$. Further, P_D^F is an increasing concave function of P_F^F for many probability distributions. The exact shape of the ROC curve depends on the probability density function of *x*. We assume that *x* follows an exponential distribution. Exponential distributions, besides being analytically tractable, capture the skewed nature of threat index of trusted and untrusted sites very well[6]. If *x* for trusted and untrusted sites follow exponential distributions with parameters θ_T and θ_U, $\theta_U > \theta_T$, respectively, then we get:

$$P_D^F = \int_t^\infty \theta_U e^{-(\theta_U x)}dx = e^{-\theta_U t}, \quad P_F^F = \int_t^\infty \theta_T e^{-(\theta_T x)}dx = e^{-\theta_T t},$$

$\Rightarrow P_D^F = \left(P_F^F\right)^{r_F}$, where $r_F = \frac{\theta_T}{\theta_U}$ is between zero and one. The parameter r_F represents the design profile of the firewall. The lower the value of r_F, the better the quality of the firewall. Figure 1 shows sample ROC curves for various values of *r*. For both the firewall and the IDS, we use this power function for the ROC curve in our analysis.

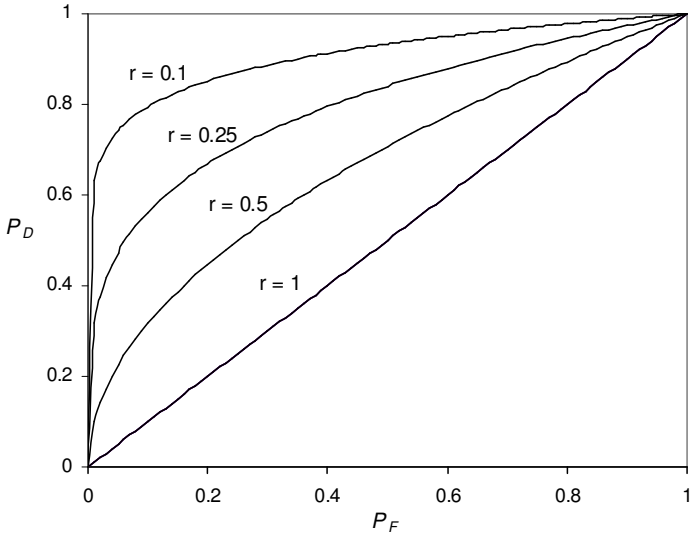

Figure 1. ROC curves for various values of *r*.

[6] Cavusoglu and Raghunathan (2004) also use exponential distributions in deriving the ROC curve for an IDS.

We make two observations regarding our modeling of the IT access and protection problem. First, a user is penalized only when the firm detects an abuse of the system. If an illegal external user attempts to gain access and is stopped by the firewall, he/she does not incur any penalty. This assumption is reasonable because we know that firewalls routinely stop numerous hacking attempts by users, and these users are not (and cannot be) penalized. Second, in our model, we normalize the payoffs such that cracking a firewall alone does not cause any damage to the firm. The firm incurs damage only when the user abuses the system, after gaining access. This assumption is reasonable because a significant proportion of intruders, known as sport hackers, is not interested in doing anything more than penetrating the firm's firewall mechanism and "take a look around" (Campbell et al. 2003, p. 242). Though the firm does not incur any direct damage when an illegal user gains access, the firm does incur an indirect cost in that an illegal user can never benefit the firm, but a legal user can. We also note that even if the firm is assumed to incur a fixed cost when an illegal user cracks the firewall, the equilibrium that we derive and our qualitative results about the value of firewall and IDS and interactions between a firewall and an IDS do not change.

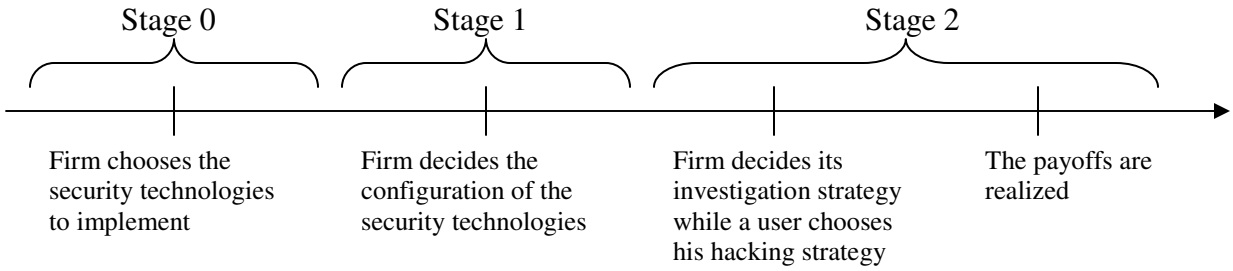

Figure 2. The timeline for the game

We model the security problem as a multi-stage game with observed actions between the firm and users of the system, as shown by the timeline given in Figure 2. First, the firm decides its security architecture, i.e., it decides whether to implement only a firewall, only an IDS, both a firewall and an IDS, or neither a firewall nor an IDS. Then, in stage 1, the firm chooses the configuration of technologies it decided to implement in stage 0. Then, given the configuration, the firm decides its manual investigation strategy while users decide their hacking strategies. Finally, the payoffs are realized. We assume that the firm and users are risk neutral. The rationale for the timeline is that configuration decisions are more strategic (long-term) and are more difficult to change compared to manual investigation strategies because changes to

software configurations often require extensive testing prior to implementation[7]. We assume that all parameters are common knowledge to all players. Thus, in stage 1 of the game, the firm decides its configuration decision by rationally anticipating its and users' optimal strategies in stage 2 of the game. In stage 2, both the firm and users observe the configuration decisions of stage 1, and simultaneously decide their strategies. Thus, we assume that in stage 2, users know whether the firm has implemented one, both, or, none of the technologies, and their configurations. This assumption is reasonable because it is well known that attackers, both internal and external, acquire knowledge about hosts and networks and their vulnerabilities using a variety of techniques including social engineering, probing, and IP fingerprinting before launching their attacks (Whitman and Mattord 2003). It is possible that internal users may have better information about the firm's decisions in stage 1 than external users. We capture this difference by assuming that internal users have perfect knowledge about firm's decisions in stage 1, but external users are uncertain about configuration decisions. An external user's belief about the firewall configuration has a probability density function $g^F(p_D^F)$ with mean equal to the true firewall configuration P_D^F and support $[\underline{P_D^F}, \overline{P_D^F}]$. Similarly, an external user's belief about the IDS configuration has a probability density function $g^I(p_D^I)$ with mean equal to the true IDS configuration P_D^I and support $[\underline{P_D^I}, \overline{P_D^I}]$. These probability functions imply that users' beliefs about configurations are unbiased.

4. Model Analysis: Equilibrium in Stage 2

We perform the analysis using backward induction. That is, first we derive the equilibrium for the firm's investigation strategy and a user's hacking strategy given the firm's implementation and configuration strategies. Note that the firm can choose to implement one, both, or none of the security technologies in stage 1 of the game. Subsequently, we determine the firm's optimal implementation and configuration strategy. The cases when the firm implements only a firewall, only an IDS, or neither a firewall nor an IDS are special cases of the more general case where the firm implements both a firewall and an IDS. Consequently, we derive the equilibrium for the firewall plus IDS case and then specialize it to other cases.

[7] For instance, in a firewall, the sequence of rules is critical in implementing a security policy, and adding, deleting, or modifying a rule could mask (contradict) other rules in a firewall. Therefore, potential contradictions have to be analyzed carefully before making a change to the firewall rule set. Such issues do not arise in the case of manual inspection strategies.

When the firm implements a firewall and an IDS, the strategy of a user that has gained access to the system, S^U, is to hack, *H*, or not hack, *NH*, i.e., $S^U \in \{H, NH\}$. The firm's strategy, S^F, is to investigate, *I*, or not investigate, *NI*, the user in each of the two states: alarm and no-alarm. That is, $S^F \in \{(I,I),(I,NI),(NI,I),(NI,NI)\}$, where the first element in each pair specifies the firm's action when the firm observes an alarm from the IDS, and the second element is the firm's action when it does not observe an alarm from the IDS. For example, (I, NI) implies that the firm investigates the user if it receives an alarm from the IDS for that user and does not investigate if it does not receive an alarm.

We derive the sub game perfect Nash equilibrium for the game between the firm and users. To do that, we first obtain the Nash equilibrium of the simultaneous game in stage 2. Let ρ_1 and ρ_2 denote the firm's investigation probabilities when the IDS raises an alarm and when the IDS does not raise an alarm, respectively. Table 2 in the Appendix provides the list of all probability expressions that are required to compute the expected payoff for the firm.

The firm's expected payoff per user in the alarm and no-alarm states given that the user gains access are given by the following:

$$F_A(\rho_1,\psi) = \omega\left(P_{I,no-hack|Alarm} + P_{E,legal,no-hack|Alarm}\right) - \rho_1 c - P_{hack|Alarm}(1-\rho_1)d - P_{hack|Alarm}\rho_1(1-\phi)d$$

$$F_{NA}(\rho_2,\psi) = \omega\left(P_{I,no-hack|No-alarm} + P_{E,legal,no-hack|No-alarm}\right) - \rho_2 c - P_{hack|No-alarm}(1-\rho_2)d - P_{hack|No-alarm}\rho_2(1-\phi)d$$

The firm's overall expected payoff per user is:

$$F(\rho_1,\rho_2,\psi) = P_{Access}\left(P_{alarm|Access}F_A(\rho_1,\psi) + P_{no-alarm|Access}F_{NA}(\rho_2,\psi)\right)$$

An internal user's payoff from hacking is given by

$$H_I(\rho_1,\rho_2,\psi) = \mu\psi - \beta(\rho_1 P_D^I + \rho_2(1-P_D^I))\psi$$

An external user's expected payoff from hacking, after gaining access, is given by

$$H_E(\rho_1,\rho_2,\psi) = \mu\psi - \beta\psi\int_{\underline{P_D^I}}^{\overline{P_D^I}} (\rho_1 p_D^I + \rho_2(1-p_D^I))g^I(p_D^I)dp_D^I = \mu\psi - \beta(\rho_1 P_D^I + \rho_2(1-P_D^I))\psi$$

The firm maximizes $F_A(\rho_1,\psi)$ when it gets an alarm from the IDS, and $F_{NA}(\rho_2,\psi)$ when it does not get an alarm from the IDS. A user maximizes his/her payoff.

The following Proposition shows the Nash equilibrium strategies for the firm and a user.

Proposition 1. *The equilibrium for stage 2 of the game when the firm implements a firewall and an IDS is given by the following.*

$$\begin{cases} \psi^* = \dfrac{cP_F^I}{d\phi P_D^I - c(P_D^I - P_F^I)}, \quad \rho_1^* = \dfrac{\mu}{P_D^I \beta}, \rho_2^* = 0 \text{ if } \dfrac{\mu}{\beta} \le P_D^I \\ \psi^* = \dfrac{c(1-P_F^I)}{c(P_D^I - P_F^I) + (1-P_D^I)d\phi}, \rho_1^* = 1, \rho_2^* = \dfrac{\mu - P_D^I \beta}{(1-P_D^I)\beta} \text{ otherwise} \end{cases}$$ ■

{The proofs for all our results are available in the Appendix}.

The equilibrium when the firm implements only a firewall, only an IDS, or neither an IDS nor a firewall can be derived from Proposition 1 by making appropriate substitutions to the firewall and IDS quality parameters. By substituting $P_D^I = P_F^I = 0$ in Proposition 1, we get the equilibrium when the firm implements only a firewall. The substitutions imply that no alarm is generated, and, by implication, no false alarm is generated. Notice that in the firewall only case, ρ_1^* is not meaningful because it represents the probability of investigation when there is an alarm. The case when the firm implements only an IDS is more complex because two possibilities arise when there is no firewall. In the first possibility, which we refer to as the *no-external-access* (NEA) scenario, the firm does not allow external access and restricts access only to internal users. In the second possibility, which we refer to as the *full-external-access* (FEA) scenario, the firm allows external access despite the absence of a firewall. The former scenario can be analyzed by setting $P_D^F = P_F^F = 1$ in our model, and the latter scenario is equivalent to substituting $P_D^F = P_F^F = 0$. For the case when the firm implements neither a firewall nor an IDS, we substitute $P_D^I = P_F^I = 0$, $\rho_1 = 0$, $\rho_2 = \rho$, and, depending on whether we model the FEA or the NEA scenario, either $P_D^F = P_F^F = 0$ (FEA) or $P_D^F = P_F^F = 1$ (NEA). Based on these substitutions, we obtain the following result.

Corollary 1. *For stage 2 of the game, (a) the equilibrium when the firm implements only the IDS, for both no-external-access and full-external-access scenarios, is identical to the equilibrium in the firewall plus IDS case given in Proposition 1, (b) the equilibria for the firewall only case and the no technology case, for both no-external-access and full-external-access scenarios, are identical and are given by the strategy profile* ($\rho^* = \mu / \beta$, $\psi^* = c / d\phi$). ■

The firm's expected payoffs under various security architectures are given in Table 3.

Table 3. Firm's Equilibrium Payoff Under Various Security Architectures

Security Architecture		**Firm's Payoff**
No Technology	NEA	$\frac{(1-\varepsilon)(\omega(d\phi-c)-cd)}{d\phi}$
	FEA	$\frac{\omega(d\phi-c)\left(1-\varepsilon(1-\zeta)\right)-cd}{d\phi}$
Firewall Only		$\frac{\omega(d\phi-c)\left(1-\varepsilon+(1-P_F^F)\varepsilon\zeta\right)-cd(1-P_D^F\varepsilon+(P_D^F-P_F^F)\varepsilon\zeta)}{d\phi}$
IDS Only	NEA	$\frac{(1-\varepsilon)(\omega(c-d\phi)P_D^I+cdP_F^I)}{(c-d\phi)P_D^I-cP_F^I}, \quad if\ \frac{\mu}{\beta}\le P_D^I$ $\frac{(1-\varepsilon)((d\phi-c)(\omega(1-P_D^I)+c(P_D^I-P_F^I))-cd(1-P_F^I))}{c(P_D^I-P_F^I)+d\phi(1-P_D^I)}, \quad if\ \frac{\mu}{\beta}>P_D^I$
	FEA	$\frac{\omega(c-d\phi)(1-\varepsilon(1-\zeta))P_D^I+cdP_F^I}{(c-d\phi)P_D^I-cP_F^I}, \quad if\ \frac{\mu}{\beta}\le P_D^I$ $\frac{(d\phi-c)(c(P_D^I-P_F^I)+\omega(1-\varepsilon(1-\zeta))(1-P_D^I))-cd(1-P_F^I)}{c(P_D^I-P_F^I)+d\phi(1-P_F^I)}, \quad if\ \frac{\mu}{\beta}>P_D^I$
IDS and Firewall		$\frac{\omega(c-d\phi)(1-\varepsilon+(1-P_F^F)\varepsilon\zeta)P_D^I+cd(1-\varepsilon P_D^F+\varepsilon\zeta(P_D^F-P_F^F))P_F^I}{(c-d\phi)P_D^I-cP_F^I}, \quad if\ \frac{\mu}{\beta}\le P_D^I$ $\frac{(c(P_D^I-P_F^I)(c-d\phi)+cd(1-P_F^F))((1-P_D^F\varepsilon)+(P_D^F-P_F^F)\varepsilon\zeta)}{-c(P_D^I-P_F^I)-d(1-P_D^I)}$ $+\frac{(c-d\phi)(1-P_D^I)w(1-\varepsilon+(1-P_F^F)\varepsilon\zeta)}{-c(P_D^I-P_F^I)-d(1-P_D^I)}, \quad if\ \frac{\mu}{\beta}>P_D^I$

It is clear from expected payoff expressions for the no technology case that the firm will allow external access even when it implements neither a firewall nor an IDS, iff $\Lambda=\frac{(c/\phi)}{\omega\zeta(1-(c/d\phi))}\le 1$. The numerator and the denominator are, respectively, the expected cost and the expected benefit from allowing access to an external user. Hence we denote the quantity Λ as the *cost-to-benefit-ratio-for-external-access*.

5. The Value of a Firewall and an IDS Under Default Configurations

We first analyze the value of a firewall and an IDS to the firm if the firm uses default configurations. That is, parameters P_D^F (hence P_F^F) and P_D^I (hence P_F^I) are exogenously

specified. Then, we consider the case when the firm chooses optimal values for these parameters in order to assess the value of configuration. We compute the value of a specific technology (or both technologies) as (firm's expected payoff when it implements a specific technology (or both technologies) – firm's expected payoff when it does not implement any technology)[8]. Even though the ROC curve for a technology relates its two quality parameters, we show them as though they are independent for clearer exposition.

5.1 The Value of Implementing Only a Firewall

Using the payoff expressions given in Table 3, we can compute the value of a firewall to be $\varepsilon\left((1-\zeta)P_D^F\left(\frac{c}{\phi}\right)-P_F^F\zeta\left(\omega\left(1-\frac{c}{d\phi}\right)-\frac{c}{\phi}\right)\right)$ for the *full-external-access* scenario and $\varepsilon\left((1-P_F^F)\omega\zeta\left(1-\frac{c}{d\phi}\right)-\left(\frac{c}{\phi}\right)\left(1-\zeta P_F^F-(1-\zeta)P_D^F\right)\right)$ for the *no-external-access* scenario. Thus, we have the following result about the value of firewall.

Proposition 2. *For the default configuration scenario, the value of implementing only a firewall is positive iff* $\frac{P_F^F}{\zeta P_F^F+(1-\zeta)P_D^F}<\Lambda<\frac{(1-P_F^F)}{\zeta\left(1-P_F^F\right)+(1-\zeta)(1-P_D^F)}$. ■

Proposition 2 shows that the firm derives a positive value from a firewall only when the *cost-to-benefit-ratio-for-external-access* is neither too high nor too low. This is intuitive because when the value of this ratio is sufficiently high, the firm will find it optimal to prohibit external access even when a firewall is available, and when the ratio has a sufficiently low value, the firm will find it desirable to allow access to every external user. In both these cases, deployment of a firewall is not preferable. Of course, the range of values for the *cost-to-benefit-ratio-for-external-access* in which the firm derives a positive value from the firewall depends on the firewall quality. A higher (lower) P_D^F (P_F^F) for the same P_F^F (P_D^F) increases the firewall quality and the range in which the firewall offers a positive value. The upper limit of the region specified in Proposition 2 represents the accuracy of the firewall in allowing external traffic, measured as the ratio of the likelihood that a legal user is allowed by the firewall to the likelihood that any external user is allowed by the firewall. The lower limit of the region represents the inaccuracy

[8] Our value analysis assumes that the cost of implementing a control is normalized to zero. This is a typical assumption in information economics (Christensen and Feltham, 2005). The idea is that a security control will not be implemented unless it is valuable.

of the firewall in dropping external traffic, measured as the ratio of the likelihood of a legal external user being dropped by the firewall to the likelihood of any external user being dropped by the firewall. Clearly, the upper limit is greater than one while the lower limit is less than one, which implies that a firewall can be beneficial to some firms that allow external traffic when they do not deploy any technology as well as to some other firms that do not allow external traffic when they do not deploy any technology.

5.2. The Value of Implementing Only an IDS

The value of IDS is given in Table 4. We highlight the significant finding as proposition 3.

Proposition 3. *For the default configuration scenario, the value of implementing only an IDS is positive iff* $(\mu/\beta) \le P_D^I$. ■

Table 4. The Value of IDS

Region	Condition(s)	The Value of IDS	Is IDS Beneficial?
$\frac{\mu}{\beta} > P_D^I$	$\Lambda < \frac{\omega\zeta(1-P_D^I)+c(P_D^I-P_F^I)}{\omega\zeta(1-P_F^I)}$	$-\frac{c(P_D^I-P_F^I)(d\phi-c)(d(1-\phi)+\omega(1-\varepsilon(1-\zeta)))}{d\phi(c(P_D^I-P_F^I)+d\phi(1-P_D^I))}$	no
	$\frac{\omega\zeta(1-P_D^I)+c(P_D^I-P_F^I)}{\omega\zeta(1-P_F^I)} < \Lambda < 1$	$-\frac{c(P_D^I-P_F^I)(d\phi-c)(1-\varepsilon)(d(1-\phi)+\omega)}{d\phi(c(P_D^I-P_F^I)+d\phi(1-P_D^I))}$ $-\frac{\varepsilon\left((d\phi-c)\omega\zeta-cd\right)}{d\phi}$	no
	$\Lambda > 1$	$-\frac{c(P_D^I-P_F^I)(d\phi-c)(1-\varepsilon)(d(1-\phi)+\omega)}{d\phi(c(P_D^I-P_F^I)+d\phi(1-P_D^I))}$	no
$\frac{\mu}{\beta} \le P_D^I$	$\Lambda < 1$	$\frac{c(P_D^I-P_F^I)(d+\omega(1-\varepsilon(1-\zeta)))(d\phi-c)}{d\phi((d\phi-c)P_D^I+cP_F^I)}$	yes
	$1 < \Lambda < \left(\frac{P_D^I}{P_F^I}\right)$	$\frac{c(P_D^I-P_F^I)(d+\omega)(1-\varepsilon)(d\phi-c)}{d\phi((d\phi-c)P_D^I+cP_F^I)}$ $+\frac{\varepsilon\left((d\phi-c)P_D^I\omega\zeta-cdP_F^I\right)}{(d\phi-c)P_D^I+cP_F^I}$	yes
	$\Lambda > \left(\frac{P_D^I}{P_F^I}\right)$	$\frac{c(P_D^I-P_F^I)(d+\omega)(1-\varepsilon)(d\phi-c)}{d\phi((d\phi-c)P_D^I+cP_F^I)}$	yes

Proposition 3 shows that an IDS that uses its default configuration does not always generate a positive value for the firm. To gain further insight into this result, we isolate the impacts of different effects on the IDS value. An IDS affects the equilibrium in two ways. First, it alters the firm's probability of manual investigation by allowing more targeted investigation. Second, it changes the users' hacking probability by altering the probability of a hacker getting caught. We can write the value of IDS as the following.

$$F^*_{IDS}(\rho^*_1, \rho^*_2, \psi^*_{IDS}) - F^*_{No-IDS}(\rho^*, \psi^*_{No-IDS}) =$$
$$\left[F^*_{IDS}(\rho^*_1, \rho^*_2, \psi^*_{No-IDS}) - F^*_{No-IDS}(\rho^*, \psi^*_{No-IDS})\right] + \left[F^*_{IDS}(\rho^*_1, \rho^*_2, \psi^*_{IDS}) - F^*_{IDS}(\rho^*_1, \rho^*_2, \psi^*_{No-IDS})\right]$$

The first term on the right-hand side of the above equation represents the increase in the firm's payoff if the firm alters its investigation strategy but users do not alter their hacking strategy after implementing the IDS. The second term represents the increase in the firm's payoff when users alter their hacking strategy in response to the change in firm's investigation strategy. Clearly, the first term incorporates the impact of the direct effect arising from targeted investigations, which, we denote as the *detection effect* of the IDS. The second term incorporates the impact of the indirect (or strategic) effect arising from the change in hacking probability, which we denote as the *deterrence effect* of IDS. An analysis of these two effects on the value of IDS shows that the detection effect is positive for all parameter values, which implies that targeted investigations enabled by the IDS always helps the firm. However, the deterrence effect is positive, i.e., the IDS reduces the probability of hacking only when $\frac{\mu}{\beta} \leq P^I_D$. When $\frac{\mu}{\beta} > P^I_D$, the deployment of an IDS increases the probability of hacking, and the loss from the higher level of hacking offsets the benefit from improved detection, which, in turn, hurts the firm.

Another important question is whether the implementation of an IDS has any impact on the firm's decision to allow or deny external access. The following result answers this question.

Corollary 2. *When the firm implements only an IDS, it will allow external access iff* $\Lambda < \frac{P^I_D}{P^I_F}$. ■

We noted in Section 4 that when the firm implements neither a firewall nor an IDS, it will allow external access when $\Lambda < 1$. Because $P^I_F < P^I_D$, in the region $1 < \Lambda < \frac{P^I_D}{P^I_F}$, the firm switches its policy from disallowing external access to one of allowing external access because of the IDS.

The reason for this result is that the improved detection enabled by IDS deters hackers, which, in turn, decreases the cost of allowing external access.

5.3. The Value of Implementing both a Firewall and an IDS

The expression for the value of firewall and IDS combination is complex. Therefore, we include it in the Appendix. However, an analysis of the expression reveals several insights into the interaction between an IDS and a firewall. The key research question that we address here is how the presence of one technology affects the value obtained from the other technology. We let V_x = Value of technology x when deployed alone, and V_{x+y} = Value of technologies x and y when deployed together. Then the interaction between technologies x and y can be categorized into three types as defined below.

Complementary: Technologies x and y are *complementary* if $V_{x+y} > \text{Max}(V_x, V_y)$ and $V_{x+y} > \text{Max}(0,V_x)+\text{Max}(0,V_y)$.

Substitutes: Technologies x and y are *substitutes* if $V_{x+y} \geq \text{Max}(V_x, V_y)$ and $V_{x+y} \leq \text{Max}(0,V_x)+\text{Max}(0,V_y)$.

Conflicting: Technologies x and y are *conflicting* if $V_{x+y} < \text{Max}(V_x, V_y)$.

The definition of complementary technologies implies that deploying both technologies results in a higher value than deploying only one of them and, further, that the incremental value offered by a technology is greater when the firm deploys the other technology than when it does not. In case of substitutes, while deploying both technologies still results in a higher value than deploying only one of them, the incremental value obtained from a technology is less when the firm deploys the other technology as well. Finally, when the technologies are conflicting, deployment of both technologies hurts the firm, i.e., the firm realizes the greatest value by deploying only one of the technologies. Now, we present one of the most significant results of this study, which describes the interaction between the values of firewall and IDS technologies with default configurations.

Proposition 4.

(1) *When* $\dfrac{\mu}{\beta} \leq P_D^I$

- *If* $\left(\dfrac{P_F^F}{\zeta P_F^F + (1-\zeta)P_D^F}\right)\left(\dfrac{P_D^I}{P_F^I}\right) < \Lambda < Min\left\{\dfrac{P_D^I}{P_F^I}, Max\left\{\left(\dfrac{P_F^F}{\zeta P_F^F + (1-\zeta)P_D^F}\right)\left(\dfrac{P_D^I}{P_F^I}\right), \dfrac{1-P_F^F}{\zeta(1-P_F^F)+(1-\zeta)(1-P_D^F)}\right\}\right\}$,

  then IDS and firewall <u>substitute</u> each other.

- *If*

$$Min\left\{\frac{P_D^I}{P_F^I}, Max\left\{\left(\frac{P_F^F}{\zeta P_F^F + (1-\zeta)P_D^F}\right)\left(\frac{P_D^I}{P_F^I}\right), \frac{1-P_F^F}{\zeta(1-P_F^F)+(1-\zeta)(1-P_D^F)}\right\}\right\} < \Lambda < \left(\frac{1-P_F^F}{\zeta(1-P_F^F)+(1-\zeta)(1-P_D^F)}\right)\left(\frac{P_D^I}{P_F^I}\right)$$

  then IDS and firewall <u>complement</u> each other.

- *Otherwise, IDS and firewall <u>conflict</u> with each other.*

(2) *When* $\frac{\mu}{\beta} > P_D^I$*: IDS and firewall <u>conflict</u> with each other.* ■

Proposition 4 can be shown graphically as Figure 3. First, the very significant result in Proposition 4 is that deploying both a firewall and an IDS can be worse for a firm than deploying only one of them. The conflict effect always occurs when one of them has a negative value, which is not completely surprising because the technology that has the negative value diminishes the value of the other technology when both are deployed together. However, a surprising finding is that the IDS and the firewall may conflict with each other even when each has a positive value individually. This scenario occurs in the region where $\frac{\mu}{\beta} \le P_D^I$ and $\left(\frac{P_F^F}{\zeta P_F^F + (1-\zeta)P_D^F}\right) < \Lambda < \left(\frac{P_F^F}{\zeta P_F^F + (1-\zeta)P_D^F}\right)\left(\frac{P_D^I}{P_F^I}\right)$. The explanation for the conflict between the firewall and the IDS in this region is as follows. If the firm does not deploy an IDS, then the firm finds that controlling the external access with the help of a firewall is valuable. However, when the firm deploys an IDS, the deterrence effect of the IDS reduces the hacking probability, which, in turn, makes allowing unfettered external access more desirable than controlled access using a firewall. In this scenario, deploying a firewall and controlling external access conflicts with the IDS. In essence, an IDS, which is traditionally viewed as a detective control, serves as an access control because of its strategic effect on hackers. When the access control function of an IDS conflicts with that of a firewall, the firm will find it optimal to use only one of them.

Second, firms that enjoy the complementary effect have a higher *cost-to-benefit-ratio-for-external-access* than firms that enjoy the substitution effect. The question of interest to security managers is why complementarity requires a higher *cost-to-benefit-ratio-for-external-access*. A firm that has a higher *cost-to-benefit-ratio-for-external-access* is less likely to allow external access if a firewall is absent. Suppose the firm does not allow external access if a firewall is absent so that the IDS receives traffic only from internal users. If the firm implements a firewall

on top of the IDS, which necessarily means that the firm allows external access, the same IDS receives a higher traffic because now it also gets traffic from external users that have been allowed by the firewall. Since the value of an IDS is directly proportional to the number of users it receives and since users do not change their strategies when a firewall is added to the security architecture, the value of IDS can only be higher in the presence of a firewall than in the absence, which indicates the complementary effect. Now consider the case in which the firm

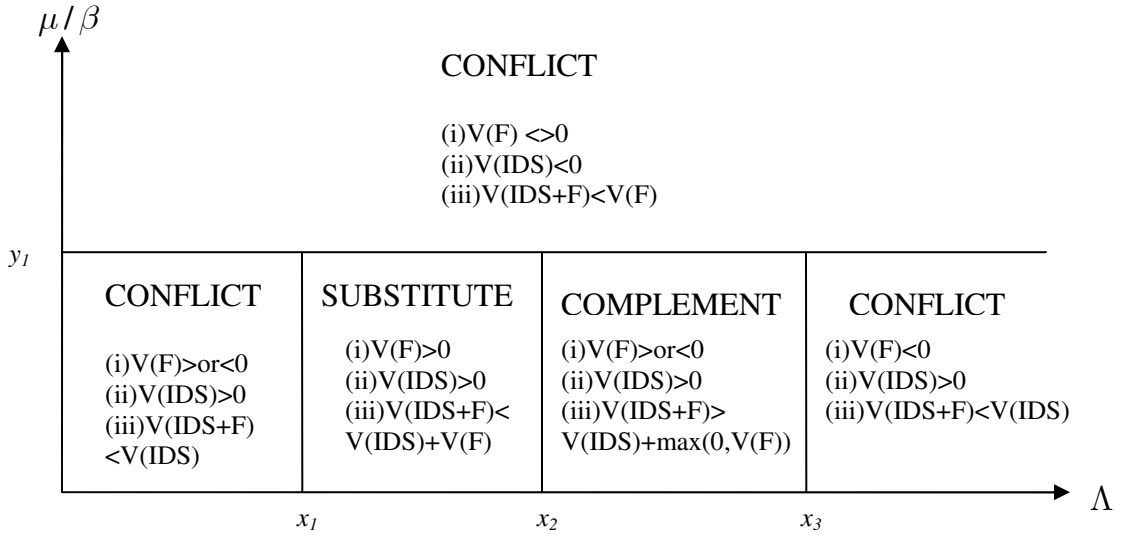

Figure 3. Interaction between a firewall and an IDS

$$\{\ y_1 = P_D^I, x_1 = \left(\frac{P_F^F}{\zeta P_F^F + (1-\zeta)P_D^F}\right)\frac{P_D^I}{P_F^I}, x_3 = \left(\frac{1-P_F^F}{\zeta(1-P_F^F)+(1-\zeta)(1-P_D^F)}\right)\frac{P_D^I}{P_F^I}\ \}$$

$$x_2 = Min\left\{\frac{P_D^I}{P_F^I}, Max\left\{\left(\frac{P_F^F}{\zeta P_F^F + (1-\zeta)P_D^F}\right)\frac{P_D^I}{P_F^I}, \frac{1-P_F^F}{\zeta(1-P_F^F)+(1-\zeta)(1-P_D^F)}\right\}\right\}$$

allows external access even without a firewall, which is likely to occur when the *cost-to-benefit-ratio-for-external-access* is sufficiently low. In this scenario, if the IDS is augmented with a firewall, the traffic to the IDS decreases because the firewall will block some of the external users. Consequently, the incremental value of the IDS is lower in the presence of a firewall than in the absence. In essence, in order for a firewall and an IDS to complement each other, each technology should perform its intended function: an IDS should act solely as a detective control and should not allow the firm to open up external access, and a firewall should act solely as an access control mechanism.

Third, we find that in the *no-external-access* scenario, a firewall that is not beneficial when deployed alone may become beneficial when deployed along with an IDS. The intuition is the following. When only a firewall is deployed, it does not offer a positive value if the expected gain from external users is less than the expected loss from hacking. An IDS with a positive value reduces the probability of hacking. This enhances the expected benefit from external users and reduces the loss from hacking. Consequently, a firewall may become beneficial when used with an IDS even if it is not beneficial when used alone.

6. Analysis of Optimal Configurations for Firewall and IDS in Stage 1

In our analysis so far, we had assumed that the firewall and IDS are implemented using their default configurations. Now, we derive the firm's optimal configurations for these technologies. Optimal configuration refers to the process of determining the best operating point (P_D^{F*} and P_F^{F*} for the firewall and P_D^{I*} and P_F^{I*} for the IDS) that maximize the value to the firm by trading off two quality parameters within the technology profiles of security controls. For both IDS and firewall, we use their respective ROC curves to identify the optimal configuration point and then compute the value of each technology at the optimal configuration point. We assume that $P_D^F = \left(P_F^F\right)^{r_F}$ and $P_D^I = \left(P_F^I\right)^{r_I}$, where $0 < r_F, r_I < 1$.

6.1 Optimally Configured Firewall

We show the following result regarding the optimal configuration when the firm implements only a firewall.

Proposition 5.

(i) When the firm finds it optimal to allow external users in the no technology case, it is optimal to deploy a firewall configured at $P_F^{F*} = \left(\frac{cdr_F(1-\zeta)}{d\phi\omega\zeta - c(d+\omega)\zeta}\right)^{\frac{1}{1-r_F}}$. *The firewall offers a non-negative value at the optimal configuration point.*

(ii) When the firm finds it optimal to disallow external users in the no technology case,

- *if* $\Lambda < \frac{1}{(r_F + (1-r_F)\zeta)}$, *it is optimal to deploy a firewall configured at* $P_F^{F*} = \left(\frac{cdr_F(1-\zeta)}{d\phi\omega\zeta - c(d+\omega)\zeta} \right)^{\frac{1}{1-r_F}}$. *The firewall offers a non-negative value at the optimal configuration point.*
- *Otherwise, it is optimal not to deploy a firewall and continue to disallow external users.* ■

Proposition 5 shows that if the firm allows external access in the absence of a firewall, then it always benefits by deploying an optimally configured firewall to control the external traffic. However, if the firm does not allow external access in the absence of a firewall, then it benefits from allowing external access and controlling the external traffic using a firewall only when cost-to-benefit-ratio-for-external-access is lower than a threshold (i.e., $\frac{1}{(r_F + (1-r_F)\zeta)}$). Since the threshold increases with firewall quality, deploying an optimally configured firewall benefits more firms if the quality is sufficiently high.

6.2 Optimally Configured IDS

We know that when $\frac{\mu}{\beta} > P_D^I$, the value of IDS is negative, and when $\frac{\mu}{\beta} < P_D^I$, the value of IDS is positive. Therefore, the firm will always configure the IDS such that the detection rate is higher than or equal to $\frac{\mu}{\beta}$, i.e., $\frac{\mu}{\beta} \le P_D^I$. We summarize the results regarding the optimal configuration of the IDS below.

Proposition 6*. When the firm implements only an IDS, the optimal configuration is given by* $P_D^{I*} = \frac{\mu}{\beta}$, *and the firm realizes a non-negative value at the optimal configuration.* ■

It is interesting to note that the firm configures the IDS at the same point irrespective of how the firm handles the external access.

6.3 Optimally Configured Firewall and IDS Combination

We know that when $(\mu/\beta) > P_D^I$, IDS and firewall conflict with each other. So, the firm configures the IDS such that $(\mu/\beta) \le P_D^I$ when the IDS is deployed together with a firewall. The optimal configuration for the firewall and IDS combination is given in the following result.

Proposition 7. *If* $\Lambda < \left(\frac{1}{r_F + (1-r_F)\zeta}\right)\left(\frac{\mu}{\beta}\right)^{\frac{r_I - 1}{r_I}}$, *the firm implements both firewall and IDS and configures them at*

$$P_D^{I*} = \frac{\mu}{\beta} \text{ and } P_D^{F*} = \left(\frac{cdr_F(1-\zeta)}{(d\phi - c)\omega\zeta\left(\frac{\mu}{\beta}\right)^{\frac{r_I - 1}{r_I}} - cd\zeta}\right)^{\frac{r_F}{1-r_F}}$$

Otherwise, the firm only implements the IDS and configures it at $P_D^{I*} = \frac{\mu}{\beta}$ *and disallows external access.* ■

The most interesting insights from Propositions 5, 6, and 7 relate to (a) how the configurations of the firewall and the IDS change when they are deployed together, compared to when they are deployed alone and (b) how optimal configuration affects the interaction between the two. We find that (i) the configuration point of the IDS does not change whether it is used alone or together with a firewall, and (ii) the firewall is configured to operate at a lower detection rate when it is used with an IDS than without, i.e., P_D^{F*} (when used alone) > P_D^{F*} (when used with an IDS). For example, suppose $r_F = 0.3$, $r_I = 0.5$, $\omega = 50$, $\zeta = 0.1$, $c = 2$, $d = 100$, $\phi = 0.5$, $\varepsilon = 0.5$, $\mu = 8$, and $\beta = 10$. We find that the optimal configuration points for the firewall when used together with an IDS and when used alone, respectively are $P_D^{F*} = 0.494$, $P_F^{F*} = 0.095$ and $P_D^{F*} = 0.548$, $P_F^{F*} = 0.134$. Knowing that there is a detective control after the firewall, the firm chooses to be less strict in allowing access, because the IDS acts as a deterrent to users that gain access. Such deterrence is absent when there is no IDS, causing the firm to be stricter in allowing access. Surprisingly, the implementation of a firewall does not change the configuration of the IDS. The reason for this result is two-fold: (i) the firewall is not a control against internal hackers, and (ii) the firewall is not a deterrent against external hackers. Unlike IDS, external

hackers are not penalized when they are stopped by a firewall, therefore they do not change their attack strategies based on the existence of a firewall. In the same vein, the strategy of internal hackers is unaffected by the firewall because they do not have to pass through the firewall. Since users' (both internal and external) hacking strategies are unaffected by the firewall configuration, and all users are identical from the IDS's perspective, the configuration of an IDS is unaffected by the firewall.

Another interesting observation from Propositions 5, 6, and 7 is that an optimally configured firewall is valuable in a larger region when it is deployed with an optimally configured IDS. So, a firm that prefers to block external access even with an optimally configured firewall may prefer to deploy the firewall instead of blocking external access when it deploys an optimally configured IDS also. The intuition is that the IDS makes the firewall more valuable due to the complementarity effect between them, as explained before.

The following result shows that how the firewall and the IDS interact with each other when they are configured optimally.

Corollary 3. *Optimally configured firewall and IDS substitute each other when*

$$\Lambda < \min\left(\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}, \left(\frac{1-P_F^{F*}}{1-(\zeta P_F^{F*}+(1-\zeta)P_D^{F*})}\right)\right) \text{ and } \underline{\text{complement}} \text{ each other when}$$

$$\min\left(\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}, \left(\frac{1-P_F^{F*}}{1-(\zeta P_F^{F*}+(1-\zeta)P_D^{F*})}\right)\right) < \Lambda < \left(\frac{1}{r_F+(1-r_F)\zeta}\right)\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}. \quad \blacksquare$$

The above result shows that optimally configured IDS and firewall **never** conflict with each other. However, even with the optimal configuration, firewall and IDS do not necessarily complement each other. An analysis of the regions in which an optimally configured firewall and an optimally configured IDS complement or substitute each other shows that an optimally configured firewall and an optimally configured IDS can complement each other only if the firm does not allow external access in the no-technology case. If the firm allows external access in the no-technology case, optimally configured IDS and firewall only substitute each other. In summary, we find that by optimally configuring an IDS and a firewall, a firm eliminates the negative effect from joint implementation of these technologies. That is, optimally-configured IDS and firewall always offer a non-negative value and never conflict with each other.

7. Robustness of Our Results: Alternative Model Specifications

In previous sections, we analyzed a model in which all users were homogenous with respect to their utility from hacking and penalty for hacking when caught. While users were classified into different types such as external versus internal and legal versus illegal, they differed only with respect to the benefit they offered to the firm. A case could be made that external hackers may incur a lower expected penalty than internal hackers because external hackers are more difficult to catch than internal hackers. Similarly, there could be differences in their utilities because the motivations of internal and external hackers are often different (Ciampa 2005). In this section, we analyze whether our results are robust to changes in our assumption about the homogeneity of users' utility and penalty parameters.

7.1 Alternative 1: Heterogeneity in Incentives to Hack between Legal and Illegal Users

In our base model, we assumed that, under normal use, the firm realizes a positive payoff only when the user is legal. The base model did not consider the payoff to a user under normal use. In many situations, a legal user conducts normal business with a firm because she has some economic payoff, and an illegal user realizes a positive economic payoff only by hacking. On the other hand, if a legal user is caught hacking, she is likely to lose her current and future payoff from the normal business, in addition to any other penalty, but an illegal user that is caught hacking suffers only from the penalty. Consequently, a legal user is likely to have less (or no) incentive to hack compared to an illegal user. We model such heterogeneity in incentives to hack between legal and illegal users by analyzing a model in which legal users do not have incentives to hack whereas illegal users decide to hack depending on their utility from hacking and penalty if caught hacking. The rest of the model remains the same as that of the base model.

We can show that all our results (Propositions 1 – 7 and Corollaries 1-3) hold qualitatively in the new model. The only differences between a result in our base model and the corresponding result in the new model relate to the expressions for the cut-off values that separate different regions. For example, the result corresponding to the interaction between a firewall and an IDS in the new model is given below.

Proposition 4B.

(1) *When* $\frac{\mu}{\beta} \le P_D^I$

- *If*

$$\frac{P_F^F\left[(d\phi-c)P_D^I+cP_F^I\right]}{\varepsilon\left[(1-\zeta)P_D^F+\zeta P_F^F\right]d\phi P_F^I} < \Lambda < Min\left\{\frac{(d\phi-c)P_D^I+cP_F^I}{d\phi P_F^I}, Max\left\{\frac{P_F^F\left[(d\phi-c)P_D^I+cP_F^I\right]}{\varepsilon\left[(1-\zeta)P_D^F+\zeta P_F^F\right]d\phi P_F^I}, \frac{1-P_F^F}{1-\varepsilon P_D^F+\varepsilon\zeta(P_D^F-P_F^F)}\right\}\right\}$$

then IDS and firewall substitute each other.

- *If*

$$Min\left\{\frac{(d\phi-c)P_D^I+cP_F^I}{d\phi P_F^I}, Max\left\{\frac{P_F^F\left[(d\phi-c)P_D^I+cP_F^I\right]}{\varepsilon\left[(1-\zeta)P_D^F+\zeta P_F^F\right]d\phi P_F^I}, \frac{1-P_F^F}{1-\varepsilon P_D^F+\varepsilon\zeta(P_D^F-P_F^F)}\right\}\right\} < \Lambda < \frac{(1-P_F^F)\left[(d\phi-c)P_D^I+cP_F^I\right]}{\left[1-\varepsilon P_D^F+\varepsilon\zeta(P_D^F-P_F^F)\right]d\phi P_F^I}$$

then IDS and firewall complement each other.

- *Otherwise, IDS and firewall conflict with each other.*

(2) *When* $\frac{\mu}{\beta} > P_D^I$*: IDS and firewall conflict with each other.*

A comparison of Proposition 4 and Proposition 4B shows that they are qualitatively identical. Similar observation applies for all other results also. Further, we confirmed that the intuition for a result in the base model and that of the corresponding result in the new model were also identical. Hence, we conclude that homogeneity in incentives of legal and illegal users does not drive our results.

7.2 Alternative 2: Heterogeneity in Incentives to Hack between Internal and External Users

We also analyzed the case in which internal and external users are heterogeneous with respect to the penalty if caught hacking. In this model, users are homogenous in all other dimensions. The primary difference between the two alternative models considered in this section is the following. In alternative 1, the hacking probability is different for legal and illegal users, but is independent of whether the user is internal or external. However, in alternative 2, the hacking probability is different for internal and external users, but is independent of whether the user is legal or illegal.

In alternative 2, the net penalty was assumed to be β and $\Delta\beta$ for an internal and an external hacker, respectively, where $0 < \Delta < 1$. Again, we found that while equilibrium strategies were different from those for the base model, our results regarding the value of firewall, value of IDS, value of firewall and IDS combination, and the nature of interaction between a firewall and an IDS in terms of complementary, substitution, and conflict effects were qualitatively identical to

those reported in our base model. However, the algebraic expressions were significantly more complex than those in the base model because hacking rates were different for external and internal users.[9] Hence, we conclude that homogeneity in incentives of internal and external users does not drive our results.

In summary, the analysis of alternative model specifications shows that all our results about the value of firewall and IDS technologies are robust and are not driven by the specific assumptions about the user behavior. Thus, we conclude that our explanations in terms of deterrence and detection effects of an IDS and access control function of a firewall and an IDS are the drivers for the results we obtained in this paper.

8. Discussion and Conclusions

The analysis presented in previous sections offered important theoretical insights into the role played by configuration on the value of IDS and firewall technologies. From a manager's perspective, important implications of our analysis pertain also to insights about the optimal firewall and IDS deployment policies. The optimal deployment policy offers guidance on when the firm should implement both a firewall and an IDS, when it should implement only an IDS, only a firewall, or neither, and whether the firm should allow external access when it does not use a firewall. These policies can be derived directly from the results stated in previous sections. We depict the optimal deployment policy graphically, as shown in Figure 4. The figure assumes that the firm configures the firewall and the IDS at their optimal configuration points. The figure reveals that a firm should implement both a firewall and an IDS when the *cost-to-benefit-ratio-for-external-access* is low. If this ratio is very low, even though the firm should implement both, the technologies substitute (imperfectly) each other. If the ratio is moderately low, then the technologies complement each other. When *cost-to-benefit-ratio-for-external-access* is sufficiently high, the firm should restrict the access only to insiders and deal with hacking that come from insiders with the help of an IDS. This result runs counter to the recommendation by some in the IT security community to rely only on firewalls for balancing the access and protection needs (Gartner 2003)[10]. We also find that optimal security architectures require implementation of both a firewall and IDS, except in a case in which the cost-to-benefit ratio of

9 For the sake of brevity, we do not reproduce the results here. The analysis of this extension is available from the authors.

[10] This result assumes that the firm configures its controls optimally before implementing them. If the firm is to deploy its security controls with default configurations, then the optimal security architecture may require the firm to implement only a firewall (see Cavusoglu, Raghunathan and Cavusoglu 2005).

external access is sufficiently high. An example for this could be military and defense systems in which the benefit from an external access is very small because the proportion of external users who are legal is very low (even though damage cost can be higher compared to other systems).

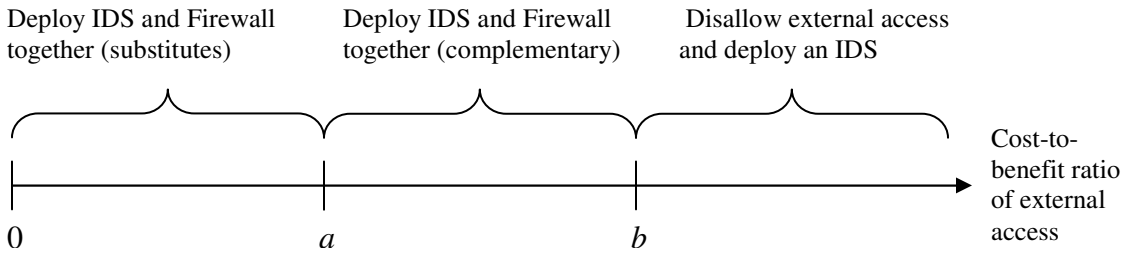

Figure 4. Design of the optimal security architecture,

$$\{\ a=\min\left[\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}},\ \left(\frac{1}{r_F+(1-r_F)\zeta}\right)\right]\ \text{and}\ b=\left(\frac{1}{r_F+(1-r_F)\zeta}\right)\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}\ \}$$

We used a stylized model for our analysis, and the model has several limitations. We assumed that the penalty is enforced as a result of hacking. This is very crucial for determining the value of an IDS. Unlike an IDS, a firewall does not require any penalty on hackers. Therefore the value of IDS can be lower in reality than what is presented here, if the enforcement of penalty is difficult. Since the value of IDS directly impacts the design of the optimal security architecture, our result about the optimal security architecture should be taken cautiously. The enforceability issue can be one of the reasons why firms consider firewalls as a mandatory technology and IDS as an optional technology in an IT security architecture. The use of default configurations may be another reason why security architectures always use a firewall.

Our model does not capture the fact that hackers may shift their resources to target different firms depending on the security controls deployed by firms. This issue was recently addressed by Cremonini and Nizovtsev (2006), who model the behavior of attackers when attackers are able to obtain complete information about the security characteristics of their targets and when such information is unavailable. They find that when attackers are able to distinguish targets by their security characteristics and switch between multiple alternative targets, the effect of a given security measure is stronger. That is due to the fact that attackers rationally put more effort into attacking systems with low security levels. Ignoring that effect would result in underinvestment in security or misallocation of security resources. Furthermore, we considered a one-shot game in our analysis. In reality, the game between a firm and hackers is a repeated one, with each party

trying to maximize its current and future periods' payoffs by observing the past. We leave this analysis to future research. Other extensions such as the impact of firm's risk profile on configuration decisions and an analysis of other functional forms for the ROC curve are also left for future research.

REFERENCES

August, T. and T. I. Tunca (2005) Network Software Security and User Incentives. *Management Science*, 52(11), pp. 1703-1720.

Axelsson, S. (2000) The Base-Rate Fallacy and the Difficulty of Intrusion Detection. *ACM Transactions on Information and System Security*, 3(3), pp. 186-205.

Campbell, P., B. Calvert and S. Boswell. (2003) *Security+ Guide to Network Security Fundamentals*, Course Technology, Boston, MA.

Cavusoglu, H. and S. Raghunathan (2004) Configuration of Detection Software: A Comparison of Decision and Game Theory Approaches. *INFORMS Decision Analysis*, 1(3), pp.131-148.

Cavusoglu, H., H. Ogut, and S. Raghunathan (2006) Intrusion Detection Policies for IT Security Breaches, *INFORMS Journal on Computing*, Forthcoming.

Cavusoglu, H. S. Raghunathan, and H. Cavusoglu (2005) How Do Security Technologies Interact With Each Other To Create Value? The Analysis of Firewall and Intrusion Detection System, *WISE*, Irvine, CA.

Cavusoglu, H., B. Mishra and S. Raghunathan. (2005) The Value of Intrusion Detection Systems (IDSs) in Information Technology Security. *Information Systems Research*, 16(1), pp. 28-46.

Cavusoglu, H., H. Cavusoglu and S. Raghunathan. (2007) Efficiency of Vulnerability Disclosure Mechanisms to Disseminate Vulnerability Knowledge. *IEEE Transactions on Software Engineering*, 33(3), pp. 171-185.

Cavusoglu, H., H. Cavusoglu and J. Zhang. (2008) Security Patch Management: Share the Burden or Share the Damage? *Management Science*, Forthcoming.

Cavusoglu, H. (2003) *The Economics of IT Security*, PhD Thesis, University of Texas at Dallas.

Christensen, P. O. and G. Feltham. (2005) Economics of Accounting – Performance Evaluation. Springer Series in Accounting Scholarship Vol. 2.

Ciampa, M. (2005). *Security+Guide to Network Security Fundamentals*, Course Technology, Boston, MA.

Cremonini M. and D. Nizovtsev. (2006) Understanding and Influencing Attackers' Decisions: Implications for Security Investment Strategies, *WEIS*, Cambridge, England.

D'haeseleer, P., S. Forrest, P. Helman. (1996) An immunological approach to change detection: Algorithms, analysis, and implications. *Proc. IEEE Sympos. Security Privacy*, pp. 110–119.

Durst, R., T. Champion, B. Witten, E. Miller, L. Spannuolo, (1999) Testing and Evaluating Computer Intrusion Detection Systems. *Communications of the ACM*. 42(7), pp. 53-61

Frincke, D., J. Evans, D. Aucutt. (1996) Hierarchical Management of Misuse Reports. *Proc. Internat. Conf. Comput. Inform.*, Ontario, Canada.

Gal-Or, E. and A. Ghose. (2005) The Economic Incentives for Sharing Security Information, *Information Systems Research*. 16(2), pp. 186-208.

Gartner. (2003) *Hype cycle for information security*. Gartner Research Report (May 30).

Garvey, T., T. Lunt. (1991) Model-based intrusion detection. *Proc. 14th National Comput. Security Conf.*, Washington, D.C.

Gigabit. (2004) Gigabit Intrusion Detection Systems. *White Paper*. Gigabit IDS Group.

Gordon, L., M. Loeb and W. Lucyshyn. (2003) Sharing Information on Computer Systems Security: An Economic Analysis**.** *Journal of Acc. and Public Policy*. 22(6), pp. 461-485.

Gouda, M. G. and Liu, X.-Y. A. (2004) Firewall design: consistency, completeness, and compactness. *24th Internat. Conf. on Distributed Computing Systems*, Tokyo, Japan.

Holden , G. (2004) *Guide to Firewalls and Network Security*. Course Technology, Boston, MA

Ilgun, K. (1992) Ustat: A real-time intrusion detection system for Unix. Master's thesis, Computer Science Department, University of California at Santa Barbara, CA.

Kumar, S., E. Spafford. (1996) A pattern matching model for misuse intrusion detection. *The COAST Project*. Purdue University, West Lafayette, IN.

Lippmann, R. P., J. W. Haines, D. J. Fried, I. Graf, J. Kobra, K. Das. (2000) The 1999 DARPA off-line intrusion detection evaluation. *Computer Networks*. 34(2), pp. 579-595

Lunt, T. (1990) Ides: An intelligent system for detecting intruders. *Proc. Sympos.: Comput. Security, Threat Countermeasures*, Rome, Italy.

Lunt, T. (1993) A survey of intrusion detection systems. *Computer Security,* 12 pp. 405–418.

Lunt, T., R. Jagannathan. (1988) A prototype real-time intrusion detection system. *Proc. 1988 IEEE Sympos. Security Privacy*, Oakland, CA.

Magalhaes, R. (2004) *Network Security recommendations that will enhance your windows network*, WindowsSecurity.com.

McCarthy, L. (1998) *Intranet Security*. Sun Microsystems Press, Santa Clara, CA.

Monrose, F., A. Rubin. (1997) Authentication via keystroke dynamics. *4th ACM Conf. Comput. Comm. Security*, Zurich, Switzerland.

Neumann, P., P. Porras. (1999) Experience with emerald to date. *Proc. 1st USENIX Workshop Intrusion Detection Network Monitoring*, Santa Clara, CA, 73–80.

Nizovtsev, D. and M. Thursby (2005). Economic analysis of incentives to disclose software vulnerabilities. *WEIS*, Boston, MA.

NMAB. (1998). *Configuration Management and Performance Verification of Explosives-Detection Systems*. Publication NMAB-482-3, National Academy Press, Washington, DC.

Ogut, H., N. Menon and S. Raghunathan. (2005) Cyber Insurance and IT Security Investment: Impact of Interdependent Risk. *WEIS*, Boston, MA

Ozment, A. (2004). Bug auctions: Vulnerability markets reconsidered. *WEIS*, Minneapolis, MN.

Piessens, F. (2002) A taxonomy of causes of software vulnerabilities in Internet software. *13th International Symposium on Software Reliability Engineering*, pp. 47-52

Porras, P., R. Kemmerer. (1992) Penetration state transition analysis: A rule-based intrusion detection approach. *IEEE 8th Annual Comput. Security Appl. Conf.*, San Antonio, TX.

Porras, P., P. Neumann. (1997) Emerald: Event monitoring enabling responses to anomalous live disturbances. *Proc. 20th Nat. Inform. Systems Security Conf.*, Baltimore, MD, 353–365.

Schechter, S. (2002) How to buy better testing: Using competition to get the most security and robustness for your dollar. *Infrastructure Security Conference*, Bristol, UK.

Trees, H. V. 2001. *Detection, Estimation and Modulation Theory-Part I*. John Wiley, New York.

Ulvila, J. W. and J. E. Gaffney. (2004) A decision analysis method for evaluating computer intrusion detection systems, *INFORMS Decision Analysis*, 1(1) pp. 35-50

Whitman, M. and H. Mattord. (2003) *Principles of Information Security*. Course Technology.

Yue, W.T. and A. Bagchi. (2003). Tuning the Quality Parameters of a Firewall to Maximize Net Benefit, Lecture Notes in Computer Science, Distributed Computing - IWDC 2003, Springer Berlin / Heidelberg, pp. 321-329

Zamboni, D., E. Spafford. (1999) New directions for the AAPHID architecture. *Workshop Recent Adv. Intrusion Detection*, West Lafayette, IN.

APPENDIX

Table 2. Probability Computations

Event	Probability Expression
a user gains access to the system	$P_{Access} = (1-\varepsilon) + \left(\varepsilon\left[(1-\zeta)(1-P_D^F) + \zeta(1-P_F^F)\right]\right)$
a user that has gained access is an internal user	$P_{I\|Access} = (1-\varepsilon) / P_{Access}$
a user that has gained access is an external legal user	$P_{E,legal\|Access} = \varepsilon\zeta(1-P_F^F) / P_{Access}$
a user that has gained access is an external illegal user	$P_{E,illegal\|Access} = \varepsilon(1-\zeta)(1-P_D^F) / P_{Access}$
a user that has gained access generates an alarm from the IDS	$P_{alarm\|Access} = P_D^I\psi + P_F^I(1-\psi)$
hack by an internal user given that IDS has generated an alarm	$P_{I,hack\|Alarm} = \frac{P_D^I\psi P_{I\|Access}}{\left(P_D^I\psi + P_F^I(1-\psi)\right)}$
normal use by an internal user given that IDS has generated an alarm	$P_{I,no-hack\|Alarm} = \frac{P_F^I(1-\psi)P_{I\|Access}}{\left(P_D^I\psi + P_F^I(1-\psi)\right)}$
hack by an external legal user given that IDS has generated an alarm	$P_{E,legal,hack\|Alarm} = \frac{P_D^I\psi P_{E,legal\|Access}}{\left(P_D^I\psi + P_F^I(1-\psi)\right)}$
normal use by an external user given that IDS has generated an alarm	$P_{E,legal,no-hack\|Alarm} = \frac{P_F^I(1-\psi)P_{E,legal\|Access}}{\left(P_D^I\psi + P_F^I(1-\psi)\right)}$
hack by an external illegal user given that IDS has generated an alarm	$P_{E,illegal,hack\|Alarm} = \frac{P_D^I\psi P_{E,illegal\|Access}}{\left(P_D^I\psi + P_F^I(1-\psi)\right)}$
normal use by an external illegal user given that IDS has generated an alarm	$P_{E,illegal,no-hack\|Alarm} = \frac{P_F^I(1-\psi)P_{E,illegal\|Access}}{\left(P_D^I\psi + P_F^I(1-\psi)\right)}$
hack by an internal user given that IDS has not generated an alarm	$P_{I,hack\|No-alarm} = \frac{(1-P_D^I)\psi P_{I\|Access}}{\left(1-P_D^I\psi - P_F^I(1-\psi)\right)}$
normal use by an internal user given that IDS has not generated an alarm	$P_{I,no-hack\|No-alarm} = \frac{(1-P_F^I)(1-\psi)P_{I\|Access}}{\left(1-P_D^I\psi - P_F^I(1-\psi)\right)}$
hack by an external legal user given that IDS has not generated an alarm	$P_{E,legal,hack\|No-alarm} = \frac{(1-P_D^I)\psi P_{E,legal\|Access}}{\left(1-P_D^I\psi - P_F^I(1-\psi)\right)}$

normal use by an external legal user given that IDS has not generated an alarm	$P_{E,legal,no-hack\|No-alarm} = \frac{(1-P_F^I)(1-\psi)P_{E,legal\|Access}}{\left(1-P_D^I\psi-P_F^I(1-\psi)\right)}$
hack by an external illegal user given that IDS has not generated an alarm	$P_{E,illegal,hack\|No-alarm} = \frac{(1-P_D^I)\psi P_{E,illegal\|Access}}{\left(1-P_D^I\psi-P_F^I(1-\psi)\right)}$
normal use by an external illegal user given that IDS has not generated an alarm	$P_{E,illegal,no-hack\|No-alarm} = \frac{(1-P_F^I)(1-\psi)P_{E,illegal\|Access}}{\left(1-P_D^I\psi-P_F^I(1-\psi)\right)}$
hack given that IDS has generated an alarm	$P_{hack\|Alarm} = P_D^I\psi / \left(P_D^I\psi + P_F^I(1-\psi)\right)$
hack given that IDS has not generated an alarm	$P_{hack\|No-alarm} = (1-P_D^I)\psi / \left(1-P_D^I\psi-P_F^I(1-\psi)\right)$

PROOFS OF RESULTS

Proof of Proposition 1

The expected payoffs for the firm in the alarm and no-alarm states and the expected payoff for the user, respectively, are:

$$F_A(\rho_1,\psi) = -\frac{\begin{bmatrix}\psi P_D^I((c\rho_1 + d(1-\rho_1\phi))(1-P_D^F\varepsilon(1-\zeta)-P_F^F\varepsilon\zeta) \\ +(1-\psi)P_F^I(c\rho_1(1-P_D^F\varepsilon(1-\zeta)-P_F^F\varepsilon\zeta)-\omega(1-\varepsilon+(1-P_F^F)\varepsilon\zeta))\end{bmatrix}}{(1-P_D^F\varepsilon(1-\zeta)-P_F^F\varepsilon\zeta)(\psi P_D^I+(1-\psi)P_F^I)} \tag{A1}$$

$$F_{NA}(\rho_2,\psi) = -\frac{\begin{bmatrix}\psi(1-P_D^I)(c\rho_2 + d(1-\rho_2\phi))(1-P_D^F\varepsilon(1-\zeta)-P_F^F\varepsilon\zeta) \\ +(1-\psi)(1-P_F^I)(\omega(1-\varepsilon+(1-P_F^F)\varepsilon\zeta)-c\rho_2(1-P_D^F\varepsilon(1-\zeta)-P_F^F\varepsilon\zeta)\end{bmatrix}}{(1-P_D^F\varepsilon(1-\zeta)-P_F^F\varepsilon\zeta)(\psi P_D^I+(1-\psi)P_F^I-1)} \tag{A2}$$

$$H(\rho_1,\rho_2,\psi) = \psi\mu - \psi\beta(\rho_1 P_D^I + \rho_2(1-P_D^I)) \tag{A3}$$

The first derivatives of payoffs with respect to the decision variables are:

$$\frac{\partial H}{\partial\psi} = \mu - \beta(\rho_1 P_D^I + \rho_2(1-P_D^I)) \tag{A4}$$

$$\frac{\partial F_A}{\partial\rho_1} = (1-P_D^F\varepsilon(1-\zeta)-P_F^F\varepsilon\zeta)(d\phi P_D^I\psi - c(P_F^I(1-\psi)+P_D^I\psi)) \tag{A5}$$

$$\frac{\partial F_{NA}}{\partial\rho_2} = (1-P_D^F\varepsilon(1-\zeta)-P_F^F\varepsilon\zeta)(d\phi(1-P_D^I)\psi - c(1-P_F^I(1-\psi)-P_D^I\psi)) \tag{A6}$$

We can verify that, for a given ψ, $\frac{\partial F_A}{\partial\rho_1} = 0$ and $\frac{\partial F_{NA}}{\partial\rho_2}$=0 cannot be satisfied simultaneously. We can also verify that $\partial F_A/\partial\rho_1 \geq \partial F_{NA}/\partial\rho_2$. Consequently, in the equilibrium, $\frac{\partial F_A}{\partial\rho_1}$>0 and $\frac{\partial F_{NA}}{\partial\rho_2}$=0, or $\frac{\partial F_A}{\partial\rho_1}$=0 and $\frac{\partial F_{NA}}{\partial\rho_2}$<0. Therefore we have two possible equilibrium scenarios: (i) $\rho_1 = 1, 0 < \rho_2 < 1$ and (ii) $0 < \rho_1 \leq 1, \rho_2 = 0$.

(i) $\rho_1 = 1, 0 < \rho_2 < 1$

In this scenario, (A4) and (A6) must be equal to zero, and (A5)>0. Solving (A4) and (A6) for ρ_2 and ψ respectively, we get

$$\rho_2^* = \frac{\mu - P_D^I\beta}{\beta(1-P_D^I)} \tag{A7}$$

$$\psi^* = \frac{c(1-P_F^I)}{c(P_D^I-P_F^I)+(1-P_D^I)d\phi} \tag{A8}$$

Since $0 < \rho_2 < 1$, we get the condition $P_D^I < \frac{\mu}{\beta} < 1$. Substituting (A8) into (A5) shows that (A5) is indeed positive.

(ii) $0 < \rho_1 \leq 1, \rho_2 = 0$

In this scenario, (A4) and (A5) must be equal to zero, and (A6)<0. Solving (A4) and (A5) for ρ_1 and ψ respectively, we get

$$\rho_1^* = \frac{\mu}{P_D^I \beta} \tag{A9}$$

$$\psi^* = \frac{cP_F^I}{d\phi P_D^I - c(P_D^I - P_F^I)} \tag{A10}$$

Since $0 < \rho_1 \leq 1$, we get the condition $0 < \frac{\mu}{\beta} \leq P_D^I$. Substituting (A10) into (A6) shows that (A6) is indeed negative.

Proof of Proposition 2

It follows from the payoff expressions given in Table 3.

Proof of Proposition 3

It follows from the value of IDS expressions given in Table 4.

The Value of Firewall and IDS Combination

From the equilibrium payoffs for the firm in no technology and firewall plus IDS cases given in Table 3, we can calculate the value of firewall and IDS combination. However the expressions for the value of firewall and IDS combination are complex. Instead we compare the value of firewall and IDS combination with the value of firewall only and the value of IDS only in all parameter regions. This comparison gives us the following table. Please note that (Value of IDS) and (Value of F) represent value of individual controls, and can be different in different regions.

Table A1. The Value of IDS and Firewall in Combination

Region	Condition(s)	Value of IDS+F	Comparison
$\frac{\mu}{\beta} > P_D^I$	$\Lambda < \frac{\omega\zeta(1-P_D^I)+c(P_D^I-P_F^I)}{\omega\zeta(1-P_F^I)}$	(Value of IDS) + A	(Value of IDS) < or > (Value of IDS+F) (Value of F) > (Value of IDS+F)
		(Value of F) + B	
	$\frac{\omega\zeta(1-P_D^I)+c(P_D^I-P_F^I)}{\omega\zeta(1-P_F^I)} < \Lambda < 1$	(Value of IDS) + C	
		(Value of F) + B	
	$\Lambda > 1$	(Value of IDS) + C	
		(Value of F) + B	
$\frac{\mu}{\beta} \leq P_D^I$	$\Lambda < 1$	(Value of IDS) + D	(Value of IDS) < or > (Value of IDS+F) (Value of F) < (Value of IDS+F)
		(Value of F) + E	
	$1 < \Lambda < \left(\frac{P_D^I}{P_F^I}\right)$	(Value of IDS) + D	
		(Value of F) + E	
	$\Lambda > \left(\frac{P_D^I}{P_F^I}\right)$	(Value of IDS) + F	
		(Value of F) + E	

$$A = \frac{\varepsilon(cd(1-P_F^I) - c(d\phi - c)(P_D^I - P_F^I))(P_D^F(1-\zeta) + P_F^F\zeta) - (d\phi - c)\omega\varepsilon\zeta(1-P_D^I)P_F^F}{c(P_D^I - P_F^I) + d\phi(1-P_D^I)}$$

$$B = \frac{-c(P_D^I - P_F^I)(d\phi - c)(d(1-\varepsilon(P_D^F(1-\zeta) + P_F^F\zeta))(1-\phi) + \omega(1-\varepsilon(1-\zeta(1-P_F^F))))}{d\phi(c(P_D^I - P_F^I) + d\phi(1-P_D^I))}$$

$$C= \frac{-\varepsilon(cd(1-P_F^I)-c(d\phi-c)(P_D^I-P_F^I))(1-P_D^F(1-\zeta)-P_F^F\zeta)+(d\phi-c)\omega\varepsilon\zeta(1-P_D^I)(1-P_F^F)}{c(P_D^I-P_F^I)+d\phi(1-P_D^I)}$$

$$D= \frac{cd\varepsilon P_F^I(P_D^F(1-\zeta)+P_F^F\zeta)-(d\phi-c)\omega\varepsilon\zeta P_D^I P_F^F}{(d\phi-c)P_D^I+cP_F^I}$$

$$E= \frac{c(d\phi-c)(P_D^I-P_F^I)(d(1-\varepsilon(P_D^F(1-\zeta)+P_F^F\zeta))+\omega(1-\varepsilon(1-\zeta(1-P_F^F))))}{d\phi((d\phi-c)P_D^I+cP_F^I)}$$

$$F= \frac{-cd\varepsilon P_F^I(1-P_D^F(1-\zeta)-P_F^F\zeta)+(d\phi-c)\omega\varepsilon\zeta P_D^I(1-P_F^F)}{(d\phi-c)P_D^I+cP_F^I}$$

Proof of Proposition 4

From Table A1, we know that when $(\mu/\beta)>P_D^I$, IDS and firewall are conflicting. Otherwise (when $(\mu/\beta)\le P_D^I$) we should investigate each region to determine the interaction effect.

Region 1: $(\Lambda<1)$

In this region, firm (i) allows all external users in no technology architecture, and (ii) allows all external users in IDS only architecture. We know that Value of (IDS+F) can be less than Value of IDS (see the comparison column in table A1). If this is the case, controls are also conflicting. Otherwise controls can complement or substitute each other. We can write the condition for {Value of (IDS+F)> Value of IDS}from Table A1 as $\Lambda>\frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I}$.

Depending on the value of $\frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I}$, there are two scenarios.

Scenario 1

$$\frac{P_D^F(1-\zeta)+P_F^F\zeta}{P_F^F}>\frac{P_D^I}{P_F^I}$$

Scenario 2

$$\frac{P_D^F(1-\zeta)+P_F^F\zeta}{P_F^F}<\frac{P_D^I}{P_F^I}$$

We can show that in region 1, {Value of (IDS+F) - Value of IDS – Value of F}<0. We also know that Value of F > 0 if $\Lambda>\frac{P_F^F}{P_D^F(1-\zeta)+P_F^F\zeta}$.

In scenario 1, Value of F>0 and Value of (F+IDS)>Value of (IDS) when $\frac{P_F^F}{P_D^F(1-\zeta)+P_F^F\zeta}\frac{P_D^I}{P_F^I}<\Lambda<1$, and Value of (F+IDS)< Value of (IDS) when $\Lambda<\frac{P_F^F}{P_D^F(1-\zeta)+P_F^F\zeta}\frac{P_D^I}{P_F^I}$. Hence, controls substitute each other when

$\frac{P_F^F}{P_D^F(1-\zeta)+P_F^F\zeta}\frac{P_D^I}{P_F^I} < \Lambda < 1$ since {Value of (IDS+F) - Value of IDS – Value of (F)}<0, and controls conflict with each other when $\Lambda < \frac{P_F^F}{P_D^F(1-\zeta)+P_F^F\zeta}\frac{P_D^I}{P_F^I}$.

In scenario 2, Value of (F+IDS)<Value of IDS when $\Lambda < 1$, and therefore, controls conflict with each other.

Region 2: ($1 < \Lambda < \left(\frac{P_D^I}{P_F^I}\right)$)

In this region, firm (i) does not allow any external user in no technology case, and (ii) allows all external users in IDS only case. From Table A1, the condition for {Value of (IDS+F)> Value of IDS} is $\Lambda > \frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I}$.

Assume that $1 < \frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I}$ (i.e., $\frac{P_D^F(1-\zeta)+P_F^F\zeta}{P_F^F} < \frac{P_D^I}{P_F^I}$)

When $\frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I} < \Lambda < \frac{P_D^I}{P_F^I}$, Value of (IDS+F)> Value of IDS. So we should evaluate {Value of (IDS+F) - Value of IDS – Value of F}) to find the interaction effect. When $1 < \Lambda < \frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I}$, Value of (IDS+F)< Value of IDS. So IDS and firewall conflict with each other.

We also know that Value of F > 0 if $\Lambda < \frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}$. Depending on the value of $\frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}$, there are three scenarios in region 2.

<u>Scenario 1:</u>

$1 < \frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)} < \frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I}$

<u>Scenario 2:</u>

$\frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I} < \frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)} < \frac{P_D^I}{P_F^I}$

<u>Scenario 3:</u>

$\frac{P_D^I}{P_F^I} < \frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}$

{Value of (IDS+F) - Value of IDS – Value of F} in region 2 is negative when

$\Lambda < \frac{P_D^I}{P_F^I} + \frac{c(P_D^I-P_F^I)(1-P_F^I)}{d\phi P_F^I} + \frac{c(P_D^I-P_F^I)(1-(1-\zeta)P_D^F-\zeta P_F^F)}{\omega\zeta\phi P_F^I}$

Since this condition is always true in region 2, we can conclude that firewall and IDS can only substitute each other when all values are positive.

In scenario 1, Value of F <0 and Value of (F+IDS)> Value of (IDS) when $\frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I} < \Lambda < \frac{P_D^I}{P_F^I}$. Therefore controls complement each other when $\frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I} < \Lambda < \frac{P_D^I}{P_F^I}$ since {Value of (IDS+F) - Value of IDS – max(0,Value of F)}>0. Controls conflict with each other when $\omega\zeta < \frac{cd}{d\phi - c} < \omega\zeta \frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I}$.

In scenario 2, Value of F >0 and Value of (F+IDS)> Value of (IDS) when $\frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I} < \Lambda < \frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}$, and Value of F <0 and Value of (F+IDS)> Value of (IDS) when $\omega\zeta \frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)} < \frac{cd}{d\phi - c} < \omega\zeta \frac{P_D^I}{P_F^I}$, and Value of F >0 and Value of (F+IDS)< Value of (IDS) when $\omega\zeta < \frac{cd}{d\phi - c} < \omega\zeta \frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I}$.Therefore, controls substitute each other when $\frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I} < \Lambda < \frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}$ since {Value of (IDS+F) - Value of IDS – Value of F)}<0. Controls complement each other when $\frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)} < \Lambda < \frac{P_D^I}{P_F^I}$ since (Value of (IDS+F) - Value of IDS – max{0,Value of F}) >0. Finally controls conflict with each other when $1 < \Lambda < \frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I}$.

In scenario 3, Value of F >0 and Value of (F+IDS)> Value of (IDS) when $\frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I} < \Lambda < \frac{P_D^I}{P_F^I}$, and Value of F >0 and Value of (F+IDS)< Value of (IDS) when $1 < \Lambda < \frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I}$. Therefore controls substitute each other when $\frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I} < \Lambda < \frac{P_D^I}{P_F^I}$. Controls conflict with each other when $1 < \Lambda < \frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I}$.

Assume that $1 > \frac{P_F^F P_D^I}{(P_D^F(1-\zeta)+P_F^F\zeta)P_F^I}$ (i.e., $\frac{P_D^F(1-\zeta)+P_F^F\zeta}{P_F^F} > \frac{P_D^I}{P_F^I}$)

Again depending on the value of $\frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}$, there are two additional scenarios in region 2.

Scenario 4:

$$\frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)} < \frac{P_D^I}{P_F^I}$$

Scenario 5:

$$\frac{P_D^I}{P_F^I} < \frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}$$

In scenario 4, Value of F <0 and Value of (F+IDS)> Value of (IDS) when $\frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)} < \Lambda < \frac{P_D^I}{P_F^I}$, and Value of F >0 and Value of (F+IDS)> Value of (IDS) when $1 < \Lambda < \frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}$. Hence controls complement each other when $\frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)} < \Lambda < \frac{P_D^I}{P_F^I}$ since {Value of (IDS+F) - Value of IDS – max(0,Value of F)}>0. Controls substitute each other when $1 < \Lambda < \frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}$ since {Value of (IDS+F) - Value of IDS – Value of F)}<0**.**

In scenario 5, Value of F >0 and Value of (F+IDS)> Value of (IDS). Therefore controls always substitute each other since {Value of (IDS+F) - Value of IDS – Value of F)}<0**.**

Region 3: $(\Lambda > \left(\frac{P_D^I}{P_F^I}\right))$

In this region, the firm (i) does not allow any external user in no technology case, and (ii) does not allow any external user in IDS only case. From Table A1, the condition for {Value of (IDS+F)> Value of IDS} is $\Lambda < \frac{(1-P_F^F)P_D^I}{(1-P_D^F(1-\zeta)-P_F^F\zeta)P_F^I}$.

Since $\frac{(1-P_F^F)P_D^I}{(1-P_D^F(1-\zeta)-P_F^F\zeta)P_F^I} > \frac{P_D^I}{P_F^I}$, we can say that when $\frac{P_D^I}{P_F^I} < \Lambda < \frac{(1-P_F^F)P_D^I}{(1-P_D^F(1-\zeta)-P_F^F\zeta)P_F^I}$, Value of (IDS+F)> Value of IDS. So we should evaluate the expression {Value of (IDS+F) - Value of IDS – Value of F}}) to find the interaction effect. When $\Lambda > \frac{(1-P_F^F)P_D^I}{(1-P_D^F(1-\zeta)-P_F^F\zeta)P_F^I}$, Value of (IDS+F)< Value of IDS. So IDS and firewall conflict with each other. We also know that Value of F > 0 if $\Lambda < \frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}$. Depending on the value of $\frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}$, there are two scenarios in region 3.

Scenario 1:

$$\frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)} < \frac{P_D^I}{P_F^I}$$

Scenario 2:

$$\frac{P_D^I}{P_F^I} < \frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)} < \frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}\frac{P_D^I}{P_F^I}$$

We can show that {Value of (IDS+F) - Value of IDS – Value of F} in region 3 is positive. Therefore firewall and IDS can only complement each other when all costs are positive.

In scenario 1, Value of F <0 and Value of (F+IDS)> Value of (IDS) when $\frac{P_D^I}{P_F^I} < \Lambda < \frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}\frac{P_D^I}{P_F^I}$, and Value of F <0 and Value of (F+IDS)< Value of (IDS) when $\frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}\frac{P_D^I}{P_F^I} < \Lambda$. Therefore, controls complement each other when $\frac{P_D^I}{P_F^I} < \Lambda < \frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}\frac{P_D^I}{P_F^I}$ since {Value of (IDS+F) - Value of IDS – Max{0,Value of F}}>0. Controls conflict with each other when $\frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}\frac{P_D^I}{P_F^I} < \Lambda$.

In scenario 2, Value of F >0 and Value of (F+IDS)> Value of (IDS) when $\frac{P_D^I}{P_F^I} < \Lambda < \frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}$, and Value of F <0 and Value of (F+IDS)> Value of (IDS) when $\frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)} < \Lambda < \frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}\frac{P_D^I}{P_F^I}$,and Value of F <0 and Value of (F+IDS)< Value of (IDS) when $\frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}\frac{P_D^I}{P_F^I} < \Lambda$. Therefore, controls complement each other when $\frac{P_D^I}{P_F^I} < \Lambda < \frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}$ since {Value of (IDS+F) - Value of IDS – Value of F)}>0. Controls again complement each other when $\frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)} < \Lambda < \frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}\frac{P_D^I}{P_F^I}$ since {Value of (IDS+F) - Value of IDS – Max{0,Value of F}}>0. Finally controls conflict with each other when $\frac{(1-P_F^F)}{(1-P_D^F(1-\zeta)-P_F^F\zeta)}\frac{P_D^I}{P_F^I} < \Lambda$.

Although there are five possibilities depending on the value of firewall and IDS quality parameters, in all of these five possibilities, the transitions of interaction effects is the same. That is, the order of interaction effect from left to right is

CONFLICT->SUBSTITUTE->COMPLEMENT->CONFLICT

After carefully looking at threshold values that separate interaction effects in five possibilities, we can write the interaction results as in proposition 4

Proof of Proposition 5

(i) All-external-access scenario

Substituting $\left(P_F^F\right)^{r_F}$ for P_D^F in the value of firewall expression, we get

$\frac{cd\left(P_F^F\right)^{r_F}\varepsilon(1-\zeta)+P_F^F\varepsilon\zeta(c(d+\omega)-d\omega\phi)}{d\phi}$. Taking a partial derivative of this expression with respect to P_F^F and equating it to zero gives $P_F^{F*}=\left(\frac{cdr_F(1-\zeta)}{d\phi\omega\zeta-c(d+\omega)\zeta}\right)^{\frac{1}{1-r_F}}$. Therefore $P_D^{F*}=\left(\frac{cdr_F(1-\zeta)}{d\phi\omega\zeta-c(d+\omega)\zeta}\right)^{\frac{r_F}{1-r_F}}$. Since both P_F^{F*} and P_D^{F*} must be between zero and one, we have the following conditions.

$\Lambda<\frac{1}{\zeta}$ and $\Lambda<\frac{1}{r_F+(1-r_F)\zeta}$

Both of these conditions are satisfied all the time in the all-external-access scenario. In addition, since $\partial^2(.)/\partial\left(P_F^F\right)^2<0$, the above solutions constitute the optimal configuration point. The value at the optimal configuration point is always non-negative since the value expression is an increasing concave function.

(ii) No-external-access scenario

Substituting $\left(P_F^F\right)^{r_F}$ for P_D^F in the value of firewall expression, we get

$\varepsilon\left((1-P_F^F)\omega\zeta\left(1-\frac{c}{d\phi}\right)-\left(\frac{c}{\phi}\right)\left(1-\zeta P_F^F-(1-\zeta)\left(P_F^F\right)^{r_F}\right)\right)$. Taking a partial derivative of this expression with respect to P_F^F and equating it to zero gives $P_F^{F*}=\left(\frac{cdr_F(1-\zeta)}{d\phi\omega\zeta-c(d+\omega)\zeta}\right)^{\frac{1}{1-r_F}}$.

Therefore $P_D^{F*}=\left(\frac{cdr_F(1-\zeta)}{d\phi\omega\zeta-c(d+\omega)\zeta}\right)^{\frac{r_F}{1-r_F}}$. Since both P_F^{F*} and P_D^{F*} must be between zero and one, we have the following conditions.

$\Lambda<\frac{1}{\zeta}$ and $\Lambda<\frac{1}{r_F+(1-r_F)\zeta}$.

Both of these conditions may not be satisfied in the no-external-access scenario. The stringent condition is

$\Lambda<\frac{1}{r_F+(1-r_F)\zeta}$

In addition, since $\partial^2(.)/\partial\left(P_F^F\right)^2<0$, the above solutions constitute the optimal configuration point only when $\Lambda<\frac{1}{r_F+(1-r_F)\zeta}$. The value at the optimal configuration point is always non-negative since the value expression is an increasing concave function.

When $\Lambda > \frac{1}{r_F + (1-r_F)\zeta}$, the point that maximizes the value of firewall is P_F^{F*}>1. Since value expression is an increasing concave function, the value is maximized at P_F^{F*}=1, implying that all external users must be dropped.

Proof of Proposition 6

We know that when $\frac{\mu}{\beta} > P_D^I$, the value of IDS is negative, and when $\frac{\mu}{\beta} \le P_D^I$, the value of IDS is positive. Therefore firm will always configure its IDS such that the detection rate is higher than or equal to $\frac{\mu}{\beta}$. Given $\frac{\mu}{\beta} \le P_D^I$, the firm can be in one of the three regions

(i) $\Lambda < 1$ (ii) $1 < \Lambda < \left(\frac{P_D^I}{P_F^I}\right)$ (iii) $\Lambda > \left(\frac{P_D^I}{P_F^I}\right)$

Since the condition for the firm to be in the first region is independent of P_F^I and P_D^I, the firm that is already in region 1 cannot move to another region through configuration. However if the firm is in this region it can play with IDS detection and error rates to find the best point at which the value is maximized. Assuming that $P_D^I = \left(P_F^I\right)^{r_I}$, we can rewrite the value expression in term of P_D^I, and take a partial derivative of the expression w.r.t. P_D^I, we get:

$-\frac{c\left(P_D^I\right)^{1/r_I}(1-r_I)(d+\omega(1-\varepsilon(1-\zeta)))(d\phi-c)}{r_I\left(c\left(\left(P_D^I\right)^{1/r_I}-P_D^I\right)+d\phi P_D^I\right)^2} < 0$. So the firm configures its IDS at the lowest value of P_D^I. Since $\frac{\mu}{\beta} \le P_D^I$, the optimal configuration point is $\left(P_D^{I*}, P_F^{I*}\right) = \left(\frac{\mu}{\beta}, \frac{\mu}{\beta}^{1/r_I}\right)$.

If $\Lambda > 1$, then through configuration the firm can move between (ii) and (iii).The derivative of the value of IDS in (ii) wrt P_D^I, is

$$-\frac{c\left(P_D^I\right)^{1/r_I}(1-r_I)(d+\omega(1-\varepsilon(1-\zeta)))(d\phi-c)}{r_I\left(c\left(\left(P_D^I\right)^{1/r_I}-P_D^I\right)+d\phi P_D^I\right)^2} < 0$$

The derivative of the value of IDS in (iii) w.r.t. P_D^I, is

$$-\frac{c\left(P_D^I\right)^{1/r_I}(1-r_I)(d+\omega)(1-\varepsilon)(d\phi-c)}{r_I\left(c\left(\left(P_D^I\right)^{1/r_I}-P_D^I\right)+d\phi P_D^I\right)^2} < 0$$

We know that at the boundary between regions (ii) and (iii) (i.e., $\Lambda = \left(\frac{P_D^I}{P_F^I}\right)$), Value of IDS in (ii) = Value of IDS in (iii). Since the value is decreasing function of P_D^I in both regions, and the value expression is a continuous function in regions (ii) and (iii), the firm chooses the minimum value of

P_D^I at optimal configuration. Given that $\frac{\mu}{\beta} \le P_D^I$, the optimal configuration point is $\left(P_D^{I^*}, P_F^{I^*}\right) = \left(\frac{\mu}{\beta}, \frac{\mu}{\beta}^{1/r_I}\right)$. To sum up, irrespective of the region where the firm lies in, the optimal configuration point for IDS in IDS only case is $\left(P_D^{I^*}, P_F^{I^*}\right) = \left(\frac{\mu}{\beta}, \frac{\mu}{\beta}^{1/r_I}\right)$.

Proof of Proposition 7

We know that, for a given cost-to-benefit-ratio-for-external-access, (1) the value of firewall is the same for any value of P_D^I and (2) the value of firewall plus IDS is always greater than the value of firewall when $\frac{\mu}{\beta} > P_D^I$. Therefore the firm should configure its IDS such that $\frac{\mu}{\beta} \le P_D^I$ when IDS is deployed together with firewall.

(i) When $\Lambda < 1$ (i.e., when the firm finds it optimal to allow all external users in no technology case)

Value of (IDS+F) =

Value of IDS+ $\frac{cd\varepsilon P_F^I (P_D^F(1-\zeta) + P_F^F \zeta) - (d\phi - c)\omega\varepsilon\zeta P_D^I P_F^F}{(d\phi - c)P_D^I + cP_F^I}$

or

Value of F+ $\frac{c(d\phi - c)(P_D^I - P_F^I)(d(1-\varepsilon(P_D^F(1-\zeta) + P_F^F\zeta)) + \omega(1-\varepsilon(1-\zeta(1-P_F^F))))}{d\phi((d\phi - c)P_D^I + cP_F^I)}$

Substituting the value of either firewall or IDS when it is used alone in that region gives

Value of (IDS+F) =

$$\frac{c(d + \omega(1-\varepsilon(1-\zeta)))}{d\phi} - \frac{cP_F^I(\omega(1-\varepsilon+(1-P_F^F)\varepsilon\zeta) + d(1-\varepsilon(P_D^F(1-\zeta)+P_F^F\zeta)))}{(d\phi-c)P_D^I + cP_F^I} - P_F^F\omega\varepsilon\zeta$$

Writing the above value in terms of P_D^F and P_D^I by substituting $\left(P_D^F\right)^{\frac{1}{r_F}}$ for P_F^F and $\left(P_D^I\right)^{\frac{1}{r_I}}$ for P_F^I, we get the value of (IDS+F) ~ $f(P_D^F, P_D^I)$. To find the values of P_D^F and P_D^I that maximize Value of (IDS+F), we take partial derivatives as

$$\frac{\partial \text{Value of(IDS+F)}}{\partial P_D^I} = \frac{c\left(P_D^I\right)^{\frac{1}{r_I}}(1-r_I)\left(d(1-P_D^F\varepsilon) + \omega(1-\varepsilon) + d\varepsilon\zeta(P_D^F - \left(P_D^F\right)^{\frac{1}{r_F}}) + \omega\varepsilon\zeta(1-\left(P_D^F\right)^{\frac{1}{r_F}})\right)}{r_I\left((d\phi-c)P_D^I + c\left(P_D^I\right)^{\frac{1}{r_I}}\right)^2}$$

$\frac{\partial \text{Value of(IDS+F)}}{\partial P_D^I} < 0$ for any value of P_D^F. Therefore the firm tries to minimize P_D^I. Since P_D^I cannot be less than $\frac{\mu}{\beta}$, the firm configures the IDS at $(P_D^{I^*}, P_F^{I^*}) = (\frac{\mu}{\beta}, \left(\frac{\mu}{\beta}\right)^{\frac{1}{r^I}})$.

The partial derivative w.r.t. P_D^F gives

$$\frac{\partial \text{Value of(IDS+F)}}{\partial P_D^F} = \frac{cdP_D^F\left(P_D^I\right)^{\frac{1}{r_I}} r_F\varepsilon(1-\zeta) - \left(P_D^F\right)^{\frac{1}{r_F}}\varepsilon\zeta\left((d\phi-c)\omega P_D^I - cd\left(P_D^I\right)^{\frac{1}{r_I}}\right)}{P_D^F r_F\left((d\phi-c)P_D^I + c\left(P_D^I\right)^{\frac{1}{r_I}}\right)}.$$

Substituting the optimal value of P_D^I to the above expression, we get

$$\frac{cdP_D^F\left(\frac{\mu}{\beta}\right)^{\frac{1}{r_I}} r_F\varepsilon(1-\zeta) - \left(P_D^F\right)^{\frac{1}{r_F}}\varepsilon\zeta\left((d\phi-c)\omega\frac{\mu}{\beta} - cd\left(\frac{\mu}{\beta}\right)^{\frac{1}{r_I}}\right)}{P_D^F r_F\left((d\phi-c)\frac{\mu}{\beta} + c\left(\frac{\mu}{\beta}\right)^{\frac{1}{r_I}}\right)}.$$

Since $\left((d\phi-c)\omega P_D^I - cd\left(\frac{\mu}{\beta}\right)^{\frac{1}{r_I}}\right)$ is always positive in this region, there is always a P_D^F that will make the partial derivative zero. So we can conclude that

$$(P_D^{F*}, P_F^{F*}) = \left(\left(\frac{cdr_F(1-\zeta)}{(d\phi-c)\omega\zeta\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}} - cd\zeta}\right)^{\frac{r_F}{1-r_F}}, \left(\frac{cdr_F(1-\zeta)}{(d\phi-c)\omega\zeta\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}} - cd\zeta}\right)^{\frac{1}{1-r_F}}\right).$$

These probabilities must be between zero and one. The condition for that is

$$\Lambda < \left(\frac{1}{r_F + (1-r_F)\zeta}\right)\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}$$

Since this is always true in this region, there is no additional constraint for this equilibrium.

(ii) When $\Lambda > 1$ (i.e., when the firm finds it optimal to disallow all external users in no technology case)

Value of (IDS+F)

=Value of IDS+ $\frac{cd\varepsilon P_F^I(P_D^F(1-\zeta)+P_F^F\zeta) - (d\phi-c)\omega\varepsilon\zeta P_D^I P_F^F}{(d\phi-c)P_D^I + cP_F^I}$ when $1 < \Lambda < \left(\frac{P_D^I}{P_F^I}\right)$,

=Value of IDS+ $\frac{-cd\varepsilon P_F^I(1-P_D^F(1-\zeta)-P_F^F\zeta) + (d\phi-c)\omega\varepsilon\zeta P_D^I(1-P_F^F)}{(d\phi-c)P_D^I + cP_F^I}$ when $\Lambda > \left(\frac{P_D^I}{P_F^I}\right)$

and

=Value of F + $\frac{c(d\phi-c)(P_D^I - P_F^I)(d(1-\varepsilon(P_D^F(1-\zeta)+P_F^F\zeta)) + \omega(1-\varepsilon(1-\zeta(1-P_F^F))))}{d\phi((d\phi-c)P_D^I + cP_F^I)}$

Substituting the value of either firewall or IDS when it is used alone in that region gives

Value of (IDS+F) =

$$(1-P_F^F)\omega\varepsilon\zeta+\frac{c(1-\varepsilon)(d+\omega)}{d\phi}-\frac{cP_F^I(\omega(1-\varepsilon+(1-P_F^F)\varepsilon\zeta)+d(1-\varepsilon(P_D^F(1-\zeta)+P_F^F\zeta)))}{(d\phi-c)P_D^I+cP_F^I}.$$

Writing the above in terms of P_D^F and P_D^I by substituting $\left(P_D^F\right)^{\frac{1}{r_F}}$ for P_F^F and $\left(P_D^I\right)^{\frac{1}{r_I}}$ for P_F^I, we get (IDS+F) ~ $f(P_D^F, P_D^I)$. To find the values of P_D^F and P_D^I that maximize Value of (IDS+F), we take partial derivatives as,

$$\frac{\partial \text{Value of(IDS+F)}}{\partial P_D^I}=\frac{c\left(P_D^I\right)^{\frac{1}{r_I}}(1-r_I)\left(d(1-P_D^F\varepsilon)+\omega(1-\varepsilon)+d\varepsilon\zeta(P_D^F-\left(P_D^F\right)^{\frac{1}{r_F}})+\omega\varepsilon\zeta(1-\left(P_D^F\right)^{\frac{1}{r_F}})\right)}{r_I\left((d\phi-c)P_D^I+c\left(P_D^I\right)^{\frac{1}{r_I}}\right)^2}$$

which is the same expression as in (i). Therefore, firm configures the IDS at

$(P_D^{I^*}, P_F^{I^*})=(\frac{\mu}{\beta},\left(\frac{\mu}{\beta}\right)^{\frac{1}{r_I}})$.

The partial derivative w.r.t. P_D^F gives

$$\frac{\partial \text{Value of(IDS+F)}}{\partial P_D^F}=\frac{cdP_D^F\left(P_D^I\right)^{\frac{1}{r_I}}r_F\varepsilon(1-\zeta)-\left(P_D^F\right)^{\frac{1}{r_F}}\varepsilon\zeta\left((d\phi-c)\omega P_D^I-cd\left(P_D^I\right)^{\frac{1}{r_I}}\right)}{P_D^F r_F\left((d\phi-c)P_D^I+c\left(P_D^I\right)^{\frac{1}{r_I}}\right)},$$

which is the same expression as in (i).

Substituting the optimal value of P_D^I to the above expression, we get

$$\frac{cdP_D^F\left(\frac{\mu}{\beta}\right)^{\frac{1}{r_I}}r_F\varepsilon(1-\zeta)-\left(P_D^F\right)^{\frac{1}{r_F}}\varepsilon\zeta\left((d\phi-c)\omega\frac{\mu}{\beta}-cd\left(\frac{\mu}{\beta}\right)^{\frac{1}{r_I}}\right)}{P_D^F r_F\left((d\phi-c)\frac{\mu}{\beta}+c\left(\frac{\mu}{\beta}\right)^{\frac{1}{r_I}}\right)}.$$

$\left((d\phi-c)\omega P_D^I-cd\left(\frac{\mu}{\beta}\right)^{\frac{1}{r_I}}\right)$ is positive when $\Lambda<\frac{1}{\zeta}P_D^I\left(\frac{\mu}{\beta}\right)^{\frac{-1}{r_I}}$. We know that in (ii), $\Lambda>1$.

Therefore $\zeta<P_D^I\left(\frac{\mu}{\beta}\right)^{\frac{-1}{r_I}}$ must be true. We also know that $P_D^I=\frac{\mu}{\beta}$, so we get a condition

$\zeta < \left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}$, which is always true. Hence $\left((d\phi - c)\omega P_D^I - cd\left(\frac{\mu}{\beta}\right)^{\frac{1}{r_I}}\right)$ is positive when $1 < \Lambda < \frac{1}{\zeta}\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}$ and negative when $\Lambda > \frac{1}{\zeta}\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}$. When $\Lambda > \frac{1}{\zeta}\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}$, the partial derivative is always positive, implying that (P_D^{F*}, P_F^{F*})=(1, 1) since the value is an increasing concave function. So firewall configuration is not an issue in that case. The firm should not use a firewall and disallow external access. So we can conclude that

$$(P_D^{F*}, P_F^{F*}) = \left(\left(\frac{cdr_F(1-\zeta)}{(d\phi - c)\omega\zeta\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}} - cd\zeta}\right)^{\frac{r_F}{1-r_F}}, \left(\frac{cdr_F(1-\zeta)}{(d\phi - c)\omega\zeta\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}} - cd\zeta}\right)^{\frac{1}{1-r_F}}\right)$$

when $1 < \Lambda < \frac{1}{\zeta}\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}$. The condition that for these probabilities to be between zero and one is

$$\Lambda < \left(\frac{1}{r_F + (1-r_F)\zeta}\right)\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}$$

This condition may not be satisfied when $1 < \Lambda < \frac{1}{\zeta}\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}$ because $\left(\frac{1}{r_F + (1-r_F)\zeta}\right)$ is less than $\frac{1}{\zeta}$. So we should restrict the region to $1 < \Lambda < \left(\frac{1}{r_F + (1-r_F)\zeta}\right)\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}$. When $\left(\frac{1}{r_F + (1-r_F)\zeta}\right)\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}} < \Lambda < \frac{1}{\zeta}\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}$, the partial derivative is always positive, implying that (P_D^{F*}, P_F^{F*})=(1, 1) since the value function is increasing. So firewall configuration is not an issue. The firm should not use a firewall and disallow external access.

Proof of Corollary 3

We also know from proposition 7 that both IDS and firewall are deployed at their optimal configuration points when $\Lambda < \left(\frac{1}{r_F + (1-r_F)\zeta}\right)\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}$. Therefore we focus on this region to analyze the interaction effect (i.e., configurable region).

From proposition 4, we know that

- if $\Lambda < r1$, controls conflict with each other
- if $r1 < \Lambda < \min(\frac{P_D^I}{P_F^I}, \max(r1, r2))$, controls substitute each other

- if $\min(\frac{P_D^I}{P_F^I}, \max(r1, r2)) < \Lambda < r3$, controls complement each other
- if $\Lambda > r3$, controls conflict with each other

If we substitute the optimal configuration points into the expression for $r1$, we get

$$r1(\text{at optimal configuration}) = \frac{cdr_F}{(d\phi - c)\omega\zeta - cd\zeta(1-r_F)\left(\frac{\mu}{\beta}\right)^{\frac{1-r_I}{r_I}}}.$$

In the configurable region, $r1(\text{at optimal configuration})$ is *always* less than Λ. Therefore first alternative is not possible. Similarly,

$$r3(\text{at optimal configuration}) = \left(\frac{1-P_F^{F*}}{1-(1-\zeta)P_D^{F*}-\zeta P_F^{F*}}\right)\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}$$

We want to show that $\Lambda < \left(\frac{1-P_F^{F*}}{1-(1-\zeta)P_D^{F*}-\zeta P_F^{F*}}\right)\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}$ is true in the configurable region.

When $\Lambda = 0$ (i.e., at the lower limit), the inequality holds. When $\Lambda = \left(\frac{1}{r_F+(1-r_F)\zeta}\right)\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}$ (i.e., at the upper limit), the inequality also holds.

$\lim_{P_D^{F*}->1}\left(\frac{1-P_F^{F*}}{1-(1-\zeta)P_D^{F*}-P_F^{F*}\zeta}\right)\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}} = \Lambda = \left(\frac{1}{r_F+(1-r_F)\zeta}\right)\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}$. As Λ increases, $\left(\frac{1-P_F^{F*}}{1-(1-\zeta)P_D^{F*}-P_F^{F*}\zeta}\right)$ also increases, before reaching the upper limit, Λ is always less than $\left(\frac{1-P_F^{F*}}{1-(1-\zeta)P_D^{F*}-\zeta P_F^{F*}}\right)\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}$. Therefore the last alternative is not possible either.

So, optimally configured firewall and IDS can only complement or substitute each other.

Since $r1(\text{at optimal configuration}) < 1$ and $r2(\text{at optimal configuration}) > 1$, at optimal configuration, $\max(r1, r2) = r2$. Therefore, $\min(\frac{P_D^I}{P_F^I}, \max(r1, r2))$ is either $r2$ or $\frac{P_D^I}{P_F^I} = \left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}$.

We know that $\frac{P_D^I}{P_F^I}$ is greater than one and does not change with Λ. We also know that $r2(\text{at optimal configuration})$ is greater than one and increases with Λ. The maximum value of $r2(\text{at optimal configuration})$ is $\left(\frac{1}{r_F+(1-r_F)\zeta}\right)$, which is less than the maximum value of Λ in

the configurable region. Therefore both complementary and substitution effects are possible.

Since we cannot compare $\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}$ and $r2(\text{at optimal configuration})$, we have:

- Optimally configured controls <u>substitute</u> each other when

$$\Lambda < \min\left(\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}, \left(\frac{1-P_F^{F^*}}{1-(\zeta P_F^{F^*}+(1-\zeta)P_D^{F^*})}\right)\right)$$

- Optimally configured controls <u>complement</u> each other when

$$\min\left(\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}, \left(\frac{1-P_F^{F^*}}{1-(\zeta P_F^{F^*}+(1-\zeta)P_D^{F^*})}\right)\right) < \Lambda < \left(\frac{1}{r_F+(1-r_F)\zeta}\right)\left(\frac{\mu}{\beta}\right)^{\frac{r_I-1}{r_I}}$$