Preprint.
The final version is available at https://ieeexplore.ieee.org/document/7536376

Localizing Firewall Security Policies

***Abstract*—In complex networks, filters may be applied at different nodes to control how packets flow. In this paper, we study how to locate filtering functionality within a network. We show how to enforce a set of security goals while allowing maximal service subject to the security constraints. To implement our results we present a tool that given a network specification and a set of control rules automatically localizes the filters and generates configurations for all the firewalls in the network. These configurations are implemented using an extension of Mignis — an open source tool to generate firewalls from declarative, semantically explicit configurations.**

Our contributions include a way to specify security goals for how packets traverse the network; an algorithm to distribute filtering functionality to different nodes in the network to enforce a given set of security goals; and a proof that the results are compatible with a Mignis-based semantics for network behavior.

I. Introduction

Organizations have big and complicated networks. A university may have a network partitioned into dozens of subnets, separated either physically or as VLANs. Although many of those subnets are very similar, for instance in requiring similar protection, others are quite distinct, for instance those that contain the university's human resources servers. These require far tighter protection. As another example, consider a corporation: Some subnets contain public-facing machines such as web servers or email servers; others support an engineering department or a sales department; and yet others contain the process-control systems that keep a factory operating. Thus, they should be governed by entirely different policies for what network flows can reach them, and from where.

Indeed, a network is a graph, in which the packets flow over the edges, and the nodes may represent routers, end systems, and so forth. The security goals we would like to enforce reflect this graph structure. They are essentially about trajectories, i.e. about where packets travel to get where they are going. For instance, a packet that reaches the process control system in the factory should not have originated in the public internet. After all, some adversary may use it to insert a destructive command, regardless of how benign its source address header field looks when it arrives. Similarly, a packet that originates in the human resources department should not traverse the public internet en route to the sales department. It could be inspected while there, compromising information about salaries within the company. A security goal may also restrict which packets may take a particular trajectory, for instance only packet addresses to port 80 or 443 on a web server.

In this paper, we introduce an expressive way to state security goals for packet flows. A security goal involves three network areas B, R, E and a property ϕ over packets (generally of their header fields). Its semantics concerns the packet flows that begin at B; end at E; and traverse R. All packets that successfully complete such a flow must satisfy the predicate ϕ when it is present at location R. The state of a packet may change as it traverses the network, so the requirement applies to its state when reaching R; network address translation (NAT) is the main packet-changing operation that we consider in this paper. However, the IP security protocols raise similar issues.

We provide an algorithm to determine what filtering to do at the different routers in the network to enforce a given set of security goals, while allowing as rich a set of packet flows as are compatible with the policy. We also provide a rigorous semantics of network behavior that allows us to prove that our algorithm is sound. Finally, to implement our results we present a tool that, given a network specification and a set of control rules, uses this algorithm to automatically localize the filters and to generate configurations for all the firewalls in the network. These configurations are presented using `Mignis`$^+$, an extension of Mignis — an open-source tool to generate firewalls from declarative, semantically explicit configurations.

Related work: Our approach is motivated by some previous work. We are interested in the defining behavioral security specifications in a network. In [6] the authors have studied trajectory-based security goals, developing techniques to determine whether existing configurations enforce them correctly. The network graphs and their possible executions are formalized in the frame model of [7].

Zhang et al. [11] focus more on the possibly conflicts among policies at different organizational levels, and less on their consequences given the topology of the network. Our method is more general and is also designed to apply in the case of network operation that transform packets as they pass; we have particularly focused on NAT.

Kurshid et al. [8] demonstrate that it is possible, in a software defined networking context, to check dynamically if global, behavioral properties are maintained as invariants, for instance reachability for certain sorts of packets. We instead make no claims of real-time, on-line feasibility, but we offer a more systematic way to solve well-defined security problems at design time.

From a network programming language point of view some interesting work on security properties has been proposed. The first example is the Frenetic project [5], that can deal with dynamic policies, but does not address network reachability or cyclicity problems, and it is not clear how new added constructs can interact with old ones. Another very strong work, is NetKAT [3], a language is equipped with a sound

and complete equational theory. However, this language is very general and it is not specifically targeted at firewalls.

Finally, much work has been devoted to firewall analysis, e.g. Margrave [9], which again lacks the distributed behavior of the network. Some automatic tools for testing of the firewall configuration enforcement have been proposed (see, e.g., [2], [10]). These tools are very powerful in static networks, but they do neither prevent consistency problems when new rules are added in the wrong order, nor avoid completeness problems for some undefined packet rules.

Structure of the paper: In Section II we present a model of our network as frames and executions, together with the different types of nodes (i.e., routers, network regions, and end hosts), and trajectories. In Section III we define the security goals and the functionality goals. In Section IV we describe how to assign filtering functionality to routers so as to enforce a set of region control statements. We first consider the case without NAT, and we then extend it to the case of NAT. In Section V we first present `Mignis`$^+$, an extension of Mignis, and we then present a tool that given a network specification and a set of region control rules automatically localizes the filters and generates `Mignis`$^+$ configurations for all the firewalls in the network. We also describe a case study with a given network and the set of automatically generated configurations. Finally, we conclude in Section VI.

II. Network model

We model networks as *frames* and *executions* [7]. A *location* $\ell \in \mathcal{LO}$ represents a network node and is equipped with a set of traces $\mathsf{traces}(\ell)$ defining its possible local behaviors. We will use the words *location* and *node* interchangeably. A *channel* $c \in \mathcal{CH}$ allows the synchronous transmission of a message between its *endpoints* $\langle \mathsf{entry}, c\rangle$ and $\langle \mathsf{exit}, c\rangle$, and the set of all endpoints is $\mathcal{EP} = \{\mathsf{entry}, \mathsf{exit}\} \times \mathcal{CH}$. In order to simplify notation, we generally write $\mathsf{entry}(c)$ and $\mathsf{exit}(c)$ instead of $\langle \mathsf{entry}, c\rangle$ and $\langle \mathsf{exit}, c\rangle$. Each message also carries some *data* $v \in \mathcal{D}$.

A frame $\mathcal{F}$ supplies for each location $\ell \in \mathcal{LO}$, the set of endpoints $\mathsf{ends}(\ell)$ and the set of traces $\mathsf{traces}(\ell)$. A trace $t \in \mathsf{traces}(\ell)$ is a sequence of *labels* for ℓ, i.e., a sequence of pairs $(c, v) \in \mathsf{chan}(\ell) \times \mathcal{D}$ where $\mathsf{chan}(\ell) = \{c \in \mathcal{CH} \colon \mathsf{entry}(c) \in \mathsf{ends}(\ell) \text{ or } \mathsf{exit}(c) \in \mathsf{ends}(\ell)\}$. Intuitively, a label for ℓ is a pair (c, v) where v is a piece of $\mathcal{D}$ and c is a channel connected to location ℓ. We let $\mathcal{T}$ denote the set of traces. We now give the formal definition of frame:

Definition 1 (Frame [7])**.** Given domains $\mathcal{LO}, \mathcal{CH}, \mathcal{D}$, we say that $\mathcal{F} = (\mathsf{ends}, \mathsf{traces})$ is a *frame* iff, for each $\ell \in \mathcal{LO}$:

1) $\mathsf{ends}(\ell) \subseteq \mathcal{EP}$ is a set of endpoints such that
   a) $\langle e, c\rangle \in \mathsf{ends}(\ell)$ and $\langle e, c\rangle \in \mathsf{ends}(\ell')$ implies $\ell = \ell'$; and
   b) there is an ℓ such that $\mathsf{entry}(c) \in \mathsf{ends}(\ell)$ iff there is an ℓ' such that $\mathsf{exit}(c) \in \mathsf{ends}(\ell')$;
2) $\mathsf{traces}(\ell)$ is a prefix-closed set such that $t \in \mathsf{traces}(\ell)$ is a finite or infinite sequence of labels for ℓ. ///

Intuitively the definition above requires that each channel has a single entry and exit point, and both are in the frame. In adition, this definition does not require that the local behaviors $\mathsf{traces}(\ell)$ should be determined in any particular way. For readability we write:

$\mathsf{sender}(c) = \ell$ when $\mathsf{entry}(c) \in \mathsf{ends}(\ell)$ and
$\mathsf{rcpt}(c) = \ell$ when $\mathsf{exit}(c) \in \mathsf{ends}(\ell)$.

Thus $\mathsf{sender}(c)$ is the location that can send messages on c and $\mathsf{rcpt}(c)$ the location that can receive them.

Each $\mathcal{F}$ determines directed and undirected graphs.

Definition 2 (Frame graphs [7])**.** If $\mathcal{F}$ is a frame, then the *graph of* $\mathcal{F}$, written $\mathsf{gr}(\mathcal{F})$, is the directed graph (V, E) whose vertices V are the locations $\mathcal{LO}$, and such that there is an edge $(\ell_1, \ell_2) \in E$ iff, for some $c \in \mathcal{CH}$, $\mathsf{sender}(c) = \ell_1$ and $\mathsf{rcpt}(c) = \ell_2$.

The undirected graph $\mathsf{ungr}(\mathcal{F})$ has those vertices, and an undirected edge (ℓ_1, ℓ_2) whenever either (ℓ_1, ℓ_2) or (ℓ_2, ℓ_1) is in the edges of $\mathsf{gr}(\mathcal{F})$. ///

The execution model for frames relies on partially ordered sets of events. The ordering represents the *occurs before* relation, and events at a certain location ℓ are required to be totally ordered and included in $\mathsf{traces}(\ell)$. Formally:

Definition 3 (Events and Executions [7])**.** Let $\mathcal{F}$ be a frame, and let $\mathcal{E}$ be a structure $\langle E, \mathsf{chan}, \mathsf{msg}\rangle$. The elements of E are called *events*, and let $\mathcal{E}$ be equipped with the following functions:

$\mathsf{chan} \colon E \to \mathcal{CH}$ that returns the channel of each event; and
$\mathsf{msg} \colon E \to \mathcal{D}$ that returns the message passed in each event.

We say that $\mathcal{B} = (B, \preceq)$ is a *system of events*, written $\mathcal{B} \in \mathsf{ES}(\mathcal{E})$, iff

i) $B \subseteq E$;
ii) $\preceq$ is a partial ordering on B; and
iii) for every $e_1 \in B$, $\{e_0 \in B \colon e_0 \preceq e_1\}$ is finite.

Now let $\mathcal{B} = (B, \preceq)$ be a system of events and define $\mathsf{proj}(B, \ell)$ as

$$\{e \in B \colon \mathsf{sender}(\mathsf{chan}(e)) = \ell \text{ or } \mathsf{rcpt}(\mathsf{chan}(e)) = \ell\}.$$

$\mathcal{B}$ is an *execution*, written $\mathcal{B} \in \mathsf{Exc}(\mathcal{F})$, iff for every $\ell \in \mathcal{LO}$,

1) $\mathsf{proj}(B, \ell)$ is linearly ordered by $\preceq$, and
2) $\mathsf{proj}(B, \ell) \in \mathsf{traces}(\ell)$. ///

A linearly ordered set in which any element has at most finitely many predecessors is a sequence. Thus, Clause 1 and the finiteness condition (iii) ensure that $\mathsf{proj}(B, \ell)$ is a sequence. Clause 2 adds the requirement that this sequence is a trace of ℓ, for each choice of ℓ.

We often write (c, p) for any event e such that $\mathsf{chan}(e) = c$ and $\mathsf{msg}(e) = p$. Since different events may occur at different times, but involve the same data value p on the same channel c, this is strictly speaking an abuse of notation.

In this paper, the data values $\mathcal{D}$ are packets. We will refer to the source and destination addresses in a packet p as $\mathtt{sa}(p)$

and $\mathsf{da}(p)$. Packets have other familiar properties such as a protocol and—if the protocol is tcp or udp—a source port and a destination port.

A. Node behaviour

Nodes in a network can be of three types: *(i)* routers, *(ii)* network regions, and *(iii)* end hosts. Routers are connected to network regions (one or more), whereas end hosts are connected to a single network region, or possibly more than one network region when the device has multiple interfaces.

End hosts can be of two kinds: *promiscuous* or *chaste*. A promiscuous host will accept any packet sent to it, and may transmit any packet. A chaste host h has a set of IP addresses $IP(h)$, and only accepts packets with destination address $i \in IP(h)$, and only transmits packets with source address $i \in IP(h)$.

Given a network, one can easily construct a frame: the locations of the frame are the network nodes; for each (undirected) edge of the network, there is a pair of arcs, one in each direction.

We provide $\mathsf{traces}(\ell)$ for each network region, end host, and router.

Network region: A network region can only forward previously received packets. Formally: $(c_1, p_1), \ldots, (c_k, p_k) \in \mathsf{traces}(\ell)$ iff, $\forall i \in [1, k]$, if $\mathsf{sender}(c_i) = \ell$, then there exists $j < i : \mathsf{rcpt}(c_j) = \ell, p_i = p_j$. Notice that a network region does not guarantee to deliver every packet, nor to deliver it at most once.

End host: We have no constraint on traces for promiscuous hosts. For chaste ones, we require that source or destination address matches host's address for any packet it sends or receives: $(c_1, p_1), \ldots, (c_k, p_k) \in \mathsf{traces}(h)$ iff $\forall i \in [1, k] : \mathsf{sender}(c_i) = h$ implies $\mathsf{sa}(p_i) = h$ and $\mathsf{rcpt}(c_i) = h$ implies $\mathsf{da}(p_i) = h$.

Router: When r is a router, then its behavior is determined by a firewall $\mathcal{FW} : \mathcal{T} \times \mathcal{CH} \times \mathcal{CH} \times P \to \mathcal{P}(P)$. Intuitively, $\mathcal{FW}$ takes a trace $t \in \mathcal{T}$, representing the history, an input and an output channel c and c' and a packet p and returns a (possibly empty) set of translations of p. Given history t, these translations p' represent all the possible ways in which p is accepted by the firewall when p is received from c and p' is delivered to c'. Given a firewall $\mathcal{FW}$ and a routing function ρ, the behaviour of the router is determined as follows:

$$\frac{p' \in \mathcal{FW}(t, c, c', p) \qquad \rho(p') = c'}{\langle t, \sigma \rangle \rightsquigarrow \langle t.(c, p), \sigma \cup (c', p') \rangle} \ [\mathrm{filter_{in}}]$$

$$\langle t, \sigma \uplus \{(c, p)\} \rangle \rightsquigarrow \langle t.(c, p), \sigma \rangle \ [\mathrm{route_{out}}]$$

Router configuration is a pair $\langle t, \sigma \rangle$ where trace t represents the history and σ is a buffer containing pairs (c, p) representing a packet p to be delivered over channel c. Intuitively, rule $\mathrm{filter_{in}}$ accepts packet p from channel c, adding it to t, only if there exits $p' \in \mathcal{FW}(t, c, c', p)$ that will be delivered over channel c'. If this is the case, (c', p') is buffered in σ. Rule $\mathrm{route_{out}}$ takes a pair (c, p) from the buffer and delivers packet p over channel c.
We let $t \in \mathsf{traces}(r)$ iff $\langle \emptyset, \emptyset \rangle \rightsquigarrow \ldots \rightsquigarrow \langle t, \sigma \rangle$.

B. Trajectories

A *trajectory* is a path that a packet may take as it traverses the network. Since the packet itself may change as it passes through a router with Network Address Translation, we need to define which events may belong together, i.e. when the packet in a second event is the result of a NAT operation on the packet in the first event.

Definition 4. Two events e, e' are *associated* if $\mathsf{rcpt}(\mathsf{chan}(e)) = \mathsf{sender}(\mathsf{chan}(e')) = \ell$ and either

1) ℓ is a network region and $\mathsf{msg}(e) = \mathsf{msg}(e')$; or
2) ℓ is a router that allows a trace $(c_0, p_0), \ldots, (c_k, p_k)$ and $\exists i, j : i < j$ such that $(c_i, p_i) = e \wedge (c_j, p_j) = e'$, $p_j \in \mathcal{FW}(t_{i-1}, c_i, c_j, p_i)$ and $\rho(p_j) = c_j$ where $t_{i-1} = (c_0, p_0), \ldots, (c_{i-1}, p_{i-1})$. ///

The next result shows that packet association corresponds to the causal relation between inputs and outputs.

Proposition 5. Let $\ell \in \mathcal{LO}$. Then

1) If $e = (c, p), e' = (c', p')$ are associated at ℓ then there exists a trace $(c_1, p_1), \ldots, (c_k, p_k) \in \mathsf{traces}(\ell)$ such that $(c_i, p_i) = (c, p) \wedge (c_j, p_j) = (c', p') \wedge i < j$;
2) $\forall (c_1, p_1), \ldots, (c_k, p_k) \in \mathsf{traces}(\ell)$, if $\mathsf{sender}(c_j) = \ell$ then $\exists i < j : \mathsf{rcpt}(c_i) = \ell$ and $(c_i, p_i), (c_j, p_j)$ are associated at ℓ.

Proof. For item 1) Assume ℓ is a network region. Then $\mathsf{msg}(e) = p = p' = \mathsf{msg}(e')$. By the behaviour of network regions (cf. section II-A) we get that $(c, p), (c', p') \in \mathsf{traces}(\ell)$ which gives the thesis. If ℓ is a router, thesis is a direct consequence of definition 4, item 2.

Item 2) can be trivially derived by the definition of traces for network region and routers given in section II-A. □

A *trajectory* is a path that a packet may take from the point it originates through network regions and routers, possibly reaching an end host at which it is received. A trajectory is *successful* if it originates with an end host whose IP addresses include its (claimed) source address, and terminates with an end host whose IP addresses include its destination address. Thus, at the beginning it is not spoofed, and at the end it is not promiscuously received.

Definition 6. Let $\mathcal{B} \in \mathsf{Exc}(\mathcal{F})$ be an execution and let $\vec{e} = \langle e_0, \ldots e_k \rangle$ be a sequence of events in $\mathcal{B}$. We say that $\vec{e}$ is a *trajectory in* $\mathcal{B}$ iff

i) $0 \leq i < j \leq k$ implies $e_i \prec e_j$;
ii) either $\mathsf{sender}(\mathsf{chan}(e_0))$ is promiscuous, or $\mathsf{sa}(\mathsf{msg}(e_0)) \in \mathsf{IP}(\mathsf{sender}(\mathsf{chan}(e_0)))$;
iii) either $\mathsf{rcpt}(\mathsf{chan}(e_k))$ is promiscuous, or $\mathsf{da}(\mathsf{msg}(e_k)) \in \mathsf{IP}(\mathsf{rcpt}(\mathsf{chan}(e_k)))$;
iv) if $i < k$, then $\mathsf{rcpt}(\mathsf{chan}(e_i))$ is a network region or router, not an end host;

v) for all i such that $0 \leq i < k$, e_i, e_{i+1} are associated.

The trajectory $\vec{e}$ is *successful* iff

$$\begin{array}{rcl} \mathsf{sa}(\mathsf{msg}(e_0)) & \in & \mathsf{IP}(\mathsf{sender}(\mathsf{chan}(e_0))) \\ \mathsf{da}(\mathsf{msg}(e_k)) & \in & \mathsf{IP}(\mathsf{rcpt}(\mathsf{chan}(e_k))) \end{array} \quad ///$$

The purpose of course of a network is to allow trajectories to succeed whenever that is compatible with the security goals of the network administrator.

When a packet p will be unchanged throughout a trajectory, for instance because the frame involves no network address translation, we often regard a trajectory as a pair consisting of the packet p together with a path π, where a *path* is a sequence of adjacent locations.

III. Goals for Security and Functionality

A. Security Goals

We focus on *three-region policy statements* as security goals. We refer to them as *region control statements*. These take the following form, in which the region variables B, E, R each refer to end hosts and network regions, and ψ_B, ψ_E, and ϕ refer to sets of packets, determined by the header fields of the packet at that step in the trajectory:

Region control $\psi_B@B \to \phi@R \to \psi_E@E$**:** For every trajectory τ,
if τ starts at location B with a packet that satisfies ψ_B,
and τ ends at location E with a packet that satisfies ψ_E,
then if location R is traversed in τ, the packet satisfies ϕ while at R.

In these region control statements, the sets ψ_B, ψ_E restrict the applicability of the security goal: They constrain a trajectory only if they are satisfied at the beginning and end respectively. By contrast, ϕ is imposing a requirement, since the network must ensure it is satisfied when the trajectory reaches R.

We can express many useful properties by suitable choices of ϕ. For instance, we may want to ensure that a packet passing from B to E undergoes network address translation properly, so that its source address at the time it traverses R is a *routable address* rather than a private address. We may want to assure that packets from public regions B to a protected corporate region E have been *properly filtered* by the time they reach the corporate entry network R; thus, they should be `tcp` packets whose destinations are the publicly accessible web and email servers, and whose destination ports are the corresponding well-known ports. These provide examples of region control statements.

We will always assume that $B \neq E$, but there are many useful cases in which the intermediate region R equals one of the endpoints, i.e. $B = R$ or $R = E$. We refer to these as *two-region* statements, since they just restrict the packets that can travel from B to E. When $R = E$, the statement says that whenever a packet travels from B to R, it must satisfy ϕ. Generally speaking, when the purpose of the statement is to protect R from potentially harmful packets from B, this form of the statement is useful; the property ϕ specifies which packets are safe. The two-region formulas may also be used with $R = B$ to protect B against disclosure of certain packets to E. In this case, the property ϕ specifies which packets are non-sensitive.

Consider another type of security goal involving three regions:

Traversal control $\psi_B@B \twoheadrightarrow R \twoheadrightarrow \psi_E@E$**:** For every trajectory τ,
if τ starts at location B with a packet that satisfies ψ_B,
and τ ends at location E with a packet that satisfies ψ_E,
then location R is traversed in τ.

As an example of a traversal control statement, consider a corporate network that has packet inspection in a particular region R. Then we may want to ensure that packets from public sources B to internal destinations E traverse R. The reverse is also important in most cases, i.e. that packets from internal sources to public destinations should traverse R.

Given a particular network, i.e. the graph underlying a frame, one strategy to enforce a traversal control statement is using region control statements. We may select a suitable cut set C of nodes between B and E where $R \in C$. We can then implement the traversal control statement by stipulating the region control statements that for trajectories from B to E, if the packets traverse any member of $C \setminus \{R\}$, then they satisfy the always-false header property **false**. That is, we have the family of statements, one for each $R' \neq R$ in C:

$$\psi_B@B \to \mathbf{false}@R' \to \psi_E@E.$$

Given this, we will focus our attention on region control statements $\psi_B@B \to \phi@R \to \psi_E@E$.

A trajectory violates a region control statement if it has the correct beginning and end points, but violates the property ϕ while at R.

Definition 7. A trajectory $\vec{e} = \langle e_0, \ldots e_k \rangle$ is a counterexample to the region control statement $\psi_B@B \to \phi@R \to \psi_E@E$ iff

1) $\mathsf{sender}(\mathsf{chan}(e_0)) = B$ and $\psi_B(\mathsf{msg}(e_0))$;
2) $\mathsf{rcpt}(\mathsf{chan}(e_k)) = E$ and $\psi_E(\mathsf{msg}(e_k))$; and
3) for some i such that $0 \leq i \leq k$, $\neg\phi(\mathsf{msg}(e_i))$ and either $\mathsf{sender}(\mathsf{chan}(e_i)) = R$ or $\mathsf{rcpt}(\mathsf{chan}(e_i)) = R$.

When $\vec{e}$ is not a counterexample we say that $\vec{e}$ *satisfies* the region control statement $\psi_B@B \to \phi@R \to \psi_E@E$. A frame $\mathcal{F}$ *enforces* $\psi_B@B \to \phi@R \to \psi_E@E$ iff, whenever $\mathcal{B} \in \mathsf{Exc}(\mathcal{F})$ is an execution of $\mathcal{F}$ and $\vec{e}$ is a trajectory in $\mathcal{B}$, then $\vec{e}$ satisfies $\psi_B@B \to \phi@R \to \psi_E@E$. ///

B. Functionality Goals

Unlike security goals, which are mandatory, functionality may be a matter of degree. We choose to measure functionality by the set of packets that have a *successful trajectory* (Def. 6). A successful trajectory is one in which a packet travels from a non-spoofing producer to a consumer actually located at the destination address of the packet. We focus on successful trajectories because we regard spoofing originators as intrinsically hostile, which is also the case for promiscuous hosts that consume packets not addressed to them. We do not care

whether exactly the same paths are available for successful trajectories, but only that a successful trajectory shoddily exist for as many packets as possible. Thus, we define:

Definition 8. Let $\mathcal{F}_1$ and $\mathcal{F}_2$ be two frames with the same underlying graph.

$\mathcal{F}_2$ is *at least as successful functionally* as $\mathcal{F}_1$ iff, for all locations ℓ and packets p, if p has a successful trajectory starting at ℓ in $\mathcal{F}_1$, then it also has a successful trajectory starting at ℓ in $\mathcal{F}_2$. ///

Given an underlying network topology, formalized as a graph, and a set of security goals, the acceptable frames are those that allow no counterexamples to the security goals. Among those, one would like to construct a frame that is maximal in the ordering of successful functionality.

C. Forms of Goals

In the remainder of this paper, we will make an assumption about the sets of security goals we will consider. It is mere bookkeeping, since any set of goals can be rewritten as a somewhat larger set of goals satisfying this assumption.

Assumption 9. In any set of security goals to be enforced, for any of those goals $\psi_B@B \to \phi@R \to \psi_E@E$, one of the following three cases holds:

1) for all packets $p \in \psi_B$, $\mathtt{sa}(p) \in IP(B)$, and for all packets $p \in \psi_E$, $\mathtt{da}(p) \in IP(E)$;
2) for all packets $p \in \psi_B$, $\mathtt{sa}(p) \notin IP(B)$; or
3) for all packets $p \in \psi_E$, $\mathtt{da}(p) \notin IP(E)$.

We refer to these goals as (1) *success goals*, (2) *spoofing goals*, and (3) *promiscuous delivery goals* respectively. We will call goals of the second and third kind jointly *promiscuity goals*.

Success goals concern only successful trajectories in which the packet is not spoofed when created nor delivered promiscuously when consumed. Spoofing goals consider only trajectories with spoofing at creation; promiscuous delivery goals, trajectories with promiscuous delivery. The spoofing and promiscuous delivery goals overlap. Any $\psi_B@B \to \phi@R \to \psi_E@E$ splits into at most three goals, each of which applies in only one of these cases:

$$(\psi_B \wedge \mathtt{sa}(p) \in IP(B))@B \to \phi@R \to (\psi_E \wedge \mathtt{da}(p) \in IP(E))@E$$
$$(\psi_B \wedge \mathtt{sa}(p) \notin IP(B))@B \to \phi@R \to \psi_E@E$$
$$\psi_B@B \to \phi@R \to (\psi_E \wedge \mathtt{da}(p) \notin IP(E))@E$$

This decomposition is useful, because when we treat goals of the first kind, we must be careful to enforce them tightly. When preventing all counterexamples, we want to ensure that any non-counterexample that satisfies the assumptions remains possible. These are successful trajectories, and a network that filters them unnecessarily is less successful functionally than it could be.

On the other hand, promiscuity goals, i.e. goals of the second and third kind, may be enforced cavalierly. A trajectory that satisfies the assumptions but is not a counterexample may be filtered out, since it would not be a successful trajectory. Thus, no functionality is sacrificed if it is discarded.

For this reason, in this paper we will focus on identifying how to enforce the success goals precisely.

IV. Localizing Security Policies

In this section, we describe how to assign filtering functionality to routers so as to enforce a set of region control statements. For this, we will develop our method based on a well-known matrix-based algorithm. To explain it, we will start from the traditional version, which is applicable in the special case where the network has no nodes that perform NAT. If there are NAT nodes, we need represent the effect of the various NAT nodes traversed along a path as a relation that composes their individual effects. In case there are NATs, we will identify some assumptions on their network position and behavior.

A. Without Network Address Translation

When the network has no nodes configured to do network address translation, then every trajectory has the same packet throughout. Thus, only the position of the packet changes as it progresses; its headers remain the same. This leads to two simplifications. First, it is easy to compare a property of headers at one location with the effects it has at other locations; for instance, when packets not satisfying ϕ are discarded at some point of a path, the consequence is that packets reaching some subsequent point along that path satisfy ϕ. Second, non-simple paths, which may revisit the same node more than once, never create any new behavior. Since the only effect of a router may be to discard packets, the set of packets that can traverse a path is a subset of the packets that can traverse any of its subpaths. Hence if any traversal provides a counterexample to a security goal, then we may assume that it is the result of appending two simple paths, one from the beginning region B to the intermediate region R, and another from region R to the end region E. In subsequent sections we will lift these simplifications, but the backbone of our analysis will be clearer in an exposition that can rely on them.

1) Specifying which packets to keep: We focus on the success goals. Fix a particular pair of endpoints B, E. Thus, we have a collection of statements of the form $\psi_B@B \to \phi_0@R \to \psi_E@E$; because these are success goals, ψ_B, ψ_E ensure that packets contain suitable addresses:

$$\psi_B(p) \Rightarrow \mathtt{sa}(p) \in IP(B) \quad \text{and} \quad \psi_E(p) \Rightarrow \mathtt{da}(p) \in IP(E).$$

Different goals in this collection may have different choices of ψ_B and ψ_E. Since trajectories do not alter packet properties in the no-NAT case, we can equivalently rewrite them to use uniform guards by replacing them this with the equivalent form:

$$[\mathtt{sa}(p) \in IP(B)]@B \to [\psi_B \wedge \psi_E \Rightarrow \phi_0]@R \to [\mathtt{da}(p) \in IP(E)]@E$$

Thus, we have essentially moved the variability in ψ_B, ψ_E from the endpoints to R, creating a new formula ϕ_1 at R. Thus, we will now assume that all B, E goals have the same guard formulas at B and E, namely $\mathtt{sa}(p) \in IP(B)$ and $\mathtt{da}(p) \in IP(E)$. We will however keep writing ϕ for the generic form

of a formula required at the intermediate location R, even if it has been rewritten as shown above.

Fix a choice of B, E. We will write $P_{B,E}$ for the set of packets with $\mathtt{sa}(p) \in IP(B)$ and $\mathtt{da}(p) \in IP(E)$.

Definition 10. Suppose given a non-empty collection G of success goals rewritten if necessary to produce uniform ψ_B, ψ_E. We define $\mathsf{Prmt}_{B,E}(\ell)$ to be:

$$\mathsf{Prmt}_{B,E}(\ell) = P_{B,E} \cap \bigcap_{\phi_\ell} \phi_\ell,$$

taking the intersection over all of the ϕ_ℓ such that a formula $\psi_B@B \to \phi_\ell@\ell \to \psi_E@E$ appears in G. We may write $\mathsf{Prmt}(\ell)$ whenever B, E are clear from the context. ///

Thus, $\mathsf{Prmt}_{B,E}(\ell)$ always includes the packets which are permitted to appear in ℓ, as part of a successful trajectory from B to E. A packet is *worth keeping* at a location if it can use that location to get from B to E while traversing only locations at which it is permitted:

Definition 11 (Keep)**.** Packet $p \in P_{B,E}$ is *worth keeping along path* π from B to E iff, for every ℓ along π, $p \in \mathsf{Prmt}_{B,E}(\ell)$.

Packet $p \in P_{B,E}$ is *worth keeping from* B to E at ℓ iff there exists some π such that π leads from B to E and traverses ℓ, and p is worth keeping along path π.

We write $\mathsf{KEEP}_{B,E}(\ell)$ for the set of $p \in P_{B,E}$ worth keeping from B to E at ℓ. We write $\mathsf{KEEP}(\ell)$ whenever B and E are clear form the context. ///

If a packet is permitted at all locations along some path from B to E that passes through ℓ, then it is certainly permitted at location ℓ:

Lemma 12. If $p \in \mathsf{KEEP}_{B,E}(\ell)$, then $p \in \mathsf{Prmt}_{B,E}(\ell)$.

Notice that a packet going from B to E is permitted at a given location ℓ only if it does not contradict any of the possible region control rules. So, for a packet to be worth keeping from B to E, it is enough if there is a single path π in which p is allowed to traverse all locations of π.

By the second of the simplifications mentioned at the beginning of Section IV-A, this definition is unchanged whether we consider all π or only the paths π in which the part before ℓ is simple, and the part after is too.

The direct way of computing $\mathsf{KEEP}(\ell)$ would thus be to examine every simple path π_1 from B to ℓ, and every path π_2 from ℓ to E, taking an intersection of the $p \in P_{B,E}$ permitted at every step of $\pi_1 \frown \pi_2$, and combining the results via a union over all choices of π_1 and π_2. We present a simpler way using matrix multiplication in Section IV-A3.

2) Combining the keep sets for different endpoints: When we define $\mathsf{KEEP}_{B,E}$, we work only with packets $p \in P_{B,E}$. We will now assume:

Assumption 13. For all locations ℓ, ℓ', if $\ell \neq \ell'$, then $IP(\ell) \cap IP(\ell') = \emptyset$.

Hence these packets are disjoint from the packets of interest when computing any other $\mathsf{KEEP}_{B',E'}$. Thus, we may simply repeat the computation for each distinct pair B, E, accumulating the union of the KEEP sets for each ℓ.

The resulting union consists of all packets that may traverse ℓ along a successful trajectory from the stated source to the stated destination without encountering a location at which it is not permitted. Thus, we may define, for a given set of goal statements G:

$$\mathsf{KEEP}_*(\ell) = \bigcup_{B,E} \mathsf{KEEP}_{B,E}(\ell) \tag{1}$$

We would like now to filter packets as they are passing from one location to another location at which they should not be kept, i.e., we should discard the complement of $\mathsf{KEEP}_*(\ell')$ along any edge $a\colon \ell \to \ell'$. We summarize this idea in filters for the arcs $a\colon \ell \to \ell'$. Since below we use the complement, the set of packets that should be accepted along a, we formalize that as the accept filter af.

Definition 14. The *acceptance filter* af is the function from arcs to sets of packets defined $\mathsf{af}(a) = \mathsf{KEEP}_*(\ell')$, when $a : \ell \to \ell'$ is an arc from ℓ to ℓ'. We also write $\mathsf{af}(\ell, \ell')$ for $\mathsf{af}(a)$.

We define the *redundant filter* of an arc $a : \ell \to \ell'$ from ℓ to ℓ' as $\mathsf{rf}_{\ell,\ell'} = \mathsf{KEEP}_*(\ell) \cap \mathsf{KEEP}_*(\ell')$. ///

Intuitively, the difference between af and rf is that the former assumes that all firewalls cooperate while the latter reenforce filtering at each firewalls in a redundant way, which would make it more robust in case some of the firewalls are compromised.

As mentioned before, we always require that $B \neq E$ in any goal statement.

Theorem 15. Let G be a non-empty collection of success goals, for a NAT-free frame. Let $\vec{e} = \langle e_0, \ldots e_k \rangle$ be a success trajectory such that $\mathsf{sender}(\mathsf{chan}(e_0)) = B$ and $\mathsf{rcpt}(\mathsf{chan}(e_k)) = E$.

- Suppose that, if for all $0 \leq i \leq k$ and locations ℓ, ℓ', if $\mathsf{sender}(\mathsf{chan}(e_i)) = \ell$ and $\mathsf{rcpt}(\mathsf{chan}(e_i)) = \ell'$, then $\mathsf{msg}(e_i) \in \mathsf{af}(\ell, \ell')$. Then $\vec{e}$ satisfies all of the success goals $\psi_B@B \to \phi@R \to \psi_E@E$ in G.
- Suppose that, if for all $0 \leq i \leq k$ and locations ℓ, ℓ', if $\mathsf{sender}(\mathsf{chan}(e_i)) = \ell$ and $\mathsf{rcpt}(\mathsf{chan}(e_i)) = \ell'$, then $\mathsf{msg}(e_i) \in \mathsf{rf}(\ell, \ell')$. Then $\vec{e}$ satisfies all of the success goals $\psi_B@B \to \phi@R \to \psi_E@E$ in G.

Proof. First, since we are assuming that there are no NATs, we have a p such that, for all i, $\mathsf{msg}(e_i) = p$. Since $\vec{e}$ is a success trajectory, $\mathtt{sa}(p) \in IP(B)$ and $\mathtt{da}(p) \in IP(E)$.

1. First suppose that $R \neq B$. If $\vec{e}$ never traverses R, then the success goal is vacuously satisfied. So let e_i be the earliest event such that $\mathsf{rcpt}(\mathsf{chan}(e_i)) = R$. By the definition of af, $p \in \mathsf{KEEP}(R)$. By Lemma 12, $p \in \mathsf{Prmt}(R)$. So p satisfies ϕ.

If $R = B$, then we use the fact that $B \neq E$. Thus, p traverses at least one edge to $\mathsf{rcpt}(\mathsf{chan}(e_0))$. Hence, $p = \mathsf{msg}(e_0) \in \mathsf{af}(B, \mathsf{rcpt}(\mathsf{chan}(e_0)))$. By the definition, $p \in \mathsf{KEEP}(\mathsf{rcpt}(\mathsf{chan}(e_0)))$. Hence, there is at least one path π that traverses $\mathsf{rcpt}(\mathsf{chan}(e_0))$ such that $p \in \mathsf{Prmt}(\ell)$ for

every ℓ along π. But B appears at the beginning of every path (including π) from B to E. Thus, $p \in \mathsf{Prmt}(B)$, so p satisfies ϕ.

2. The preceding argument applies *a fortiori*, since $\mathsf{rf}(a) \subseteq \mathsf{af}(a)$ for every a. □

Moreover, af is maximally successful among all such. That is, any assignment of filters that permits additional successful trajectories allows counterexamples to some goal. Indeed, we prevent a successful trajectory only if that trajectory is incompatible with the security goals.

Lemma 16. Suppose that f is a function from arcs to sets of packets, and for all $a : \ell \to \ell'$, either

Case (a) $\mathsf{af}(a) \subseteq f(a)$, or else

Case (b) $\mathsf{rf}(a) \subseteq f(a)$.

Suppose that τ is a successful trajectory compatible with f but not with the selected filters af or rf. Then τ is a counterexample to some success goal.

Proof. **Assuming case (a):** Since τ is incompatible with af, it traverses some edge $a : \ell \to \ell'$ such that, letting the packet of τ be p, $p \in \mathsf{KEEP}_*(\ell)$ but $p \notin \mathsf{KEEP}_*(\ell')$. Therefore there is no path π from the start of τ to its endpoint that traverses ℓ' such that $p \in \mathsf{Prmt}(\ell_1)$ for all ℓ_1 along π.

Assuming case (b): Since τ is incompatible with rf, it traverses some edge $a : \ell \to \ell'$ such that, letting the packet of τ be p, $p \notin \mathsf{KEEP}_*(\ell)$ or $p \notin \mathsf{KEEP}_*(\ell')$. Therefore, letting ℓ'' be either ℓ or ℓ', there is no path π from the start of τ to its endpoint that traverses ℓ'' such that $p \in \mathsf{Prmt}(\ell_1)$ for all ℓ_1 along π.

Hence, in either case (a) or case (b), the sequence of locations traversed in τ is not such a path. Thus, τ is a counterexample to some goal between these endpoints. □

3) Computing the sets to keep: Observe that sets of packets form a boolean algebra, and therefore surely a ring where $\cap$ is the multiplication and $\cup$ is the addition. In particular, $\cap$ distributes over $\cup$. Thus, we can form matrices of sets, and matrix multiplication accumulates the $\cup$ of the $\cap$s of corresponding elements. I.e. if we define the inner product $\vec{a} \cdot \vec{b}$ to be:

$$\bigcup_i (a[i] \cap b[i]),$$

then the matrix multiplication $A\,B$ yields C, where $C_{ij} = \vec{a}_i \cdot \vec{b}_j$ using the i^{th} row vector of A and the j^{th} column vector of B. Let:

A be the adjacency matrix for the graph, where if there is an edge from node i to node j, then the entry A_{ij} is the top element, i.e. the set of all packets. $A_{ij} = \emptyset$ if i, j are not adjacent.

K be the diagonal matrix with entries $K_{i,i} = \mathsf{Prmt}(i)$.

We want to compute the matrices Rch^m such that each entry $\mathsf{Rch}^m_{i,j}$ is the set of $p \in P_{B,E}$ that can reach node j from node i along a path of length $\leq m$ while traversing only locations n such that $p \in \mathsf{Prmt}(n)$.

We claim:

$\mathsf{Rch}^0 = K$**,** since paths of length 0 lead only from i to i, and $K_{i,i}$ is the set of packets permitted there.

$\mathsf{Rch}^1 = K + (K\,A\,K)$**.** A path of length ≤ 1 is either empty or else it takes one step from i to an adjacent location j; moreover, the packet should satisfy $\mathsf{Prmt}(i)$ before the step and $\mathsf{Prmt}(j)$ after it.

$\mathsf{Rch}^{(2m)} = (\mathsf{Rch}^m\,\mathsf{Rch}^m)$**,** since the paths of length $\leq 2m$ are just the paths that divide into two paths of length $\leq m$, respectively ending and beginning at the same node k.

Since every (simple) path visits each node at most once, it is no longer than $|\mathcal{N}|$, the cardinality of the set of nodes. As remarked above, non-simple paths allow no additional packets, since they subject the packets to additional constraints. Thus, the sequence stabilizes by Rch^b where $b = 2^{1+\log_2 |\mathcal{N}|}$, and we define:

$\mathsf{Rch} = \mathsf{Rch}^b$ is the fixed point of Rch^m.

Observe that this computation requires $\mathcal{O}(\log_2 |\mathcal{N}|)$ matrix multiplications to reach its fixed point, and is thus tractable for large $|\mathcal{N}|$, assuming that the underlying ring operations on sets are tractable.

Lemma 17. For a configuration without NAT or other packet transformations, $\mathsf{KEEP}(i) = \mathsf{Rch}_{B,i} \cap \mathsf{Rch}_{i,E}$.

Proof. Set $\mathsf{Rch}_{B,i} \cap \mathsf{Rch}_{i,E}$ contains all packets $p \in P_{B,E}$ that can reach i from B and then E from i while traversing only locations n such that $p \in \mathsf{Prmt}_{B,E}(n)$. Thus, p belongs to $\mathsf{Rch}_{B,i} \cap \mathsf{Rch}_{i,E}$ if and only if $p \in P_{B,E}$ and there exists some π such that π leads from B to E and traverses i, and for every ℓ along π, $p \in \mathsf{Prmt}_{B,E}(\ell)$. By Definition 11 we directly obtain $\mathsf{Rch}_{B,i} \cap \mathsf{Rch}_{i,E} = \mathsf{KEEP}(i)$. □

4) Tightening given filters: Suppose we want to calculate the success filters relative to some given filters $f(e, d)$, where e is an edge, d is a direction (inbound vs. outbound), and the resulting value $f(e, d)$ is the set of packets we will permit to travel along edge e in direction d. We would like to derive maximally permissive filters that tighten the given ones and enforce the goal statements. To do so, instead of starting with the adjacency matrix A, we define A^f to have the entry $f(e, d)$ in position $A^f_{i,j}$ if edge e leads from location i to location j when traversed in direction d. Like A, it contains the empty set whenever i and j are not adjacent. The successive matrices $\mathsf{Rch}^0, \mathsf{Rch}^1, \ldots, \mathsf{Rch}^m$ are now computed as before, starting with matrix A^f.

For instance, we might like to use this idea to protect terminal networks—meaning a network segment ℓ with just one connection to the remainder of the network—from inappropriate packets. Suppose that a ℓ contains IP addresses $IP(\ell)$. Thus, the remainder of the network has the complementary set of IP addresses $\overline{IP(\ell)}$.

Then we would like to permit packets p outbound only if $\mathtt{sa}(p) \in IP(\ell)$ and $\mathtt{da}(p) \in \overline{IP(\ell)}$. We would like to permit packets p inbound only if $\mathtt{da}(p) \in IP(\ell)$ and $\mathtt{sa}(p) \in \overline{IP(\ell)}$. Edges that do not connect a terminal network retain their

original specification of allowing all packets. This leads to a useful policy A^f to start from in computing the sets Rch.

5) Firewall Configuration: We now define firewall behaviour $\mathcal{FW}$ based on the KEEP_* sets. We consider the case of nodes connected to at least one firewall or, in other words, we assume that any edge in the network has filtering capabilities.

Definition 18. For each firewall ℓ_f, consider any input and output channels c_i and c_o such that $\mathsf{rcpt}(c_i) = \ell_f$ and $\mathsf{sender}(c_o) = \ell_f$. Let ℓ_i and ℓ_o be the two locations connected to c_i and c_o, i.e., $\ell_i = \mathsf{sender}(c_i), \mathsf{rcpt}(c_o) = \ell_o$. Then we define a firewall as:

$$\mathcal{FW}_a(t, c_i, c_o, p) \triangleq \begin{cases} \{p\} & \text{if } p \in \mathsf{af}_{\ell_i,\ell_f} \cap \mathsf{af}_{\ell_f,\ell_o} \\ \{\} & \text{otherwise} \end{cases}$$

and, similarly, a *redundant* firewall as:

$$\mathcal{FW}_r(t, c_i, c_o, p) \triangleq \begin{cases} \{p\} & \text{if } p \in \mathsf{rf}_{\ell_i,\ell_f} \cap \mathsf{rf}_{\ell_f,\ell_o} \\ \{\} & \text{otherwise} \end{cases} \quad ///$$

Intuitively, a firewall without network address translation accepts a packet p whenever p is accepted on both the input and the output channels, i.e., whenever p belongs to $\mathsf{af}_{\ell_i,\ell_f} \cap \mathsf{af}_{\ell_f,\ell_o}$, or to $\mathsf{rf}_{\ell_i,\ell_f} \cap \mathsf{rf}_{\ell_f,\ell_o}$ for the redundant firewall.

Theorem 19. Let G be a non-empty collection of success goals. If each channel is connected to at least one router and the behaviour of all routers is determined by $\mathcal{FW}_a(t, c_i, c_o, p)$ or $\mathcal{FW}_r(t, c_i, c_o, p)$, then frame $\mathcal{F}$ enforces G.

Proof. Suppose that, in order to get a contradiction, the firewalls are defined as above but frame $\mathcal{F}$ *does not enforce* some goal of G. This means that there is a goal $\psi_B@B \rightarrow \phi@R \rightarrow \psi_E@E$, an execution $\mathcal{B}$ of $\mathcal{F}$, and a trajectory $\vec{e} = \langle e_0, \ldots e_k \rangle$ in $\mathcal{B}$ such that $\vec{e}$ is a counterexample for this goal. By Theorem 15, there exists $0 \leq i \leq k$ such that $\mathsf{msg}(e_i) \notin \mathsf{af}(\ell, \ell')$ and $\mathsf{msg}(e_i) \notin \mathsf{rf}(\ell, \ell')$

Recall that B and E are required to be end hosts and cannot be routers. By hypothesis we have that any edge of $\mathcal{F}$ has at least one firewall so, if the firewall is located at ℓ we consider the *incoming* event e_{i-1} (from ℓ_i to ℓ) and we obtain $\mathcal{FW}_a(t, \mathsf{chan}(e_{i-1}), \mathsf{chan}(e_i), p) = \{\}$, $\mathcal{FW}_r(t, \mathsf{chan}(e_{i-1}), \mathsf{chan}(e_i), p) = \{\}$ as $p \notin \mathsf{af}(\ell_i, \ell) \cap \mathsf{af}(\ell, \ell')$, $p \notin \mathsf{rf}(\ell_i, \ell) \cap \mathsf{rf}(\ell, \ell')$; if the firewall is located at ℓ' we consider the *outgoing* event e_{i+1} (from ℓ' to ℓ_o) and again $\mathcal{FW}_a(t, \mathsf{chan}(e_i), \mathsf{chan}(e_i + 1), p) = \{\}$ and $\mathcal{FW}_r(t, \mathsf{chan}(e_i), \mathsf{chan}(e_i + 1), p) = \{\}$, as $p \notin \mathsf{af}(\ell, \ell') \cap \mathsf{af}(\ell', \ell_o)$, $p \notin \mathsf{rf}(\ell, \ell') \cap \mathsf{rf}(\ell', \ell_o)$.

In both cases, the router behaviour defined in Section II enforces that the p is blocked hence we get a contradiction on the existence of the counterexample trajectory. □

B. Localizing with NATs

In the more general case, we use the same ideas, although with a different ring. In this case, instead of the ring of sets of packets under $\cup$ and $\cap$, we use a ring of relations on packets. The addition-like operator is again $\cup$, but the multiplication-like operator is now the relative product $R \bowtie S$ of binary relations:

$$(R \bowtie S)(x, z) \text{ iff } \exists y \,.\, R(x, y) \wedge S(y, z)$$

We will next verify that these operations do form a ring.

After that, we face two additional hurdles. First, we cannot hope to enforce goals in an exact way if different regions behind the same NAT are subjected to different security policies. By the time that packets emerge through the NAT, we cannot tell in which region they originated, and thus cannot differentiate their filtering according to their origins. Second, we need an analogue to Assumption 13, which ensured that we could compute the KEEP sets for different endpoints B, E separately, and combine the results by taking disjoint unions. Instead, we will assume that the external IP addresses of any distinct NAT devices accessible to any location R are disjoint.

1) Union and relative product form a ring: We will check that this does form a ring, although it is not a commutative ring. This suffices to allow us to use the methods we have just described. We will also point out below that—for the NAT-based packet transformations that interest us—there are simple and efficient ways to represent the relations that arise in our computations.

1) $\cup$ is associative, commutative, and has unit $\emptyset$.
2) $\bowtie$ is associative, $(R \bowtie S) \bowtie T = R \bowtie (S \bowtie T)$; and it has unit the identity relation Id, meaning $R \bowtie \mathsf{Id} = R$. The former is the equivalence:

$$\begin{array}{lll} (\exists z & . & (\exists y \,.\, R(x, y) \wedge S(y, z)) \wedge T(z, w)) \equiv \\ (\exists y & . & R(x, y) \wedge (\exists z \,.\, S(y, z) \wedge T(z, w))) \end{array}$$

   while the latter says that

$$\exists y \,.\, R(x, y) \wedge y = z \equiv R(x, z).$$

3) $\bowtie$ distributes over $\cup$:

$$\begin{array}{rcl} R \bowtie (S \cup T) & = & (R \bowtie S) \cup (R \bowtie T) \quad \text{and} \\ (S \cup T) \bowtie R & = & (S \bowtie R) \cup (T \bowtie R). \end{array}$$

   We check the former, via the definitions, distributing $\wedge$ over $\vee$:

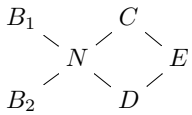
$$\begin{array}{ll} & (R \bowtie (S \cup T))(x, z) \equiv \\ \equiv & \exists y \,.\, R(x, y) \wedge (S(y, z) \vee T(y, z)) \\ \equiv & \exists y \,.\, (R(x, y) \wedge S(y, z)) \vee (R(x, y) \wedge T(y, z)) \\ \equiv & (\exists y \,.\, R(x, y) \wedge S(y, z)) \vee (\exists y \,.\, R(x, y) \wedge T(y, z)) \\ \equiv & ((R \bowtie S) \cup (R \bowtie T))(x, z) \end{array}$$

   To check the latter, we use almost the same argument, but inverting the arguments; the commutativity of $\wedge$ and $\vee$ justifies the way we write this:

$$\begin{array}{ll} & ((S \cup T) \bowtie R)(z, x) \equiv \\ \equiv & \exists y \,.\, R(y, x) \wedge (S(z, y) \vee T(z, y)) \\ \equiv & \exists y \,.\, (R(y, x) \wedge S(z, y)) \vee (R(y, x) \wedge T(z, y)) \\ \equiv & (\exists y \,.\, R(y, x) \wedge S(z, y)) \vee (\exists y \,.\, R(y, x) \wedge T(z, y)) \\ \equiv & ((R \bowtie S) \cup (R \bowtie T))(z, x) \end{array}$$

We may also regard each set of packets $\phi(p)$ as "lifting" to the binary relation $\phi(p) \wedge p = p'$, i.e. the lifted version of ϕ is the intersection $\uparrow \phi = \mathsf{Id} \cap (\phi \times \phi)$.

2) Agreeing on goals across NATs: Consider the network:



where we are interested in the packets that are permitted to travel from either B_1 or B_2 through the NAT device N to E. However, they must satisfy different properties depending on which intermediate node C, D they traverse. In particular, successful trajectories from B_1 to E that traverse C must have property ϕ, while successful trajectories from B_2 to E that traverse C must have property ψ. On the other hand, successful trajectories from B_1 to E that traverse D must have property ψ, while successful trajectories from B_2 to E that traverse D must have property ϕ.

Unfortunately, we cannot enforce this requirement before traversing the NAT N, because we do not know whether the packets will traverse the route through C or through D. And we cannot enforce this requirement after traversing the NAT N, because we do not know whether the packets originated at B_1 or B_2. N has rewritten their source addresses to its own external address.

Thus, these goals, which differentiate the packets by their source behind the NAT, cannot be enforced. Instead, all origins beyond a NAT must be subject to the same policy. Indeed, a purpose of the NAT is to make those packets indistinguishable.

In particular, consider triples of locations B_1, R, E and B_2, R, E, where R is separated from B_1, B_2 by at least one NAT. Then for every goal for B_1, R, E, there should be a goal for B_2, R, E that is at least as restrictive, and conversely. In this case, we can say that B_1, B_2 are *region of origin equi-goals* for R, E. A similar notion of *destination equi-goals* applies to E_1, E_2. A policy will be enforceable only when it ensures regions of origin and destination equi-goals across NATs.

3) Computing the matrices Rch^m*:* We regard source NAT operations as occurring outbound on an edge e, and as defined by the relation $R_e(p, p')$. Here, typically, this holds if p has a local source address; p' has the NAT device's address as its source address; and p' agrees with p for destination port and address. The translation for returning packets flowing inbound on the edge is dual.

We now construct A^f as containing these relations in entries that reflect NAT processing. If an entry reflects a filter retaining packets satisfying ϕ, then its entry is $\uparrow \phi$. The matrix K is the diagonal matrix such that $K_{i,i} = \uparrow \mathsf{Prmt}(i)$.

We now use the same scheme as before to compute the matrices Rch^m.

C. Extending to NATs

As said before, whenever we are dealing with NATs we no longer have constant packets throughout a trajectory. However, extending our plain model to NATs boils down to book-keeping these translations and evaluating the packets at each node with their current header. Luckily, the transformations we apply to packets can be described as the *relative product* operator described in the previous section.

One needs thus to adapt our notions of permitted and keep packets. For the permitted packets, we no longer require them to have their original source and detination addresses, so one defines $\mathsf{Prmt}_{B,E}(\ell) = \bigcap_{\phi_\ell} \phi_\ell$. For the definition of KEEP, we change it so that a packet is worth keeping at ℓ_i if it is worth keeping with the state that it reached ℓ_i. This definition is similar to Definition 11 replacing the occurrences of packet p and path π by $\mathsf{msg}(e_i)$ and trajectory $\vec{e}$.

Allowing the existence of NATs requires us to assume that there are two relations $\mathcal{D}D_\ell$ and $\mathcal{S}S_\ell$ for each node ℓ, that are respectively the DNAT and SNAT relations at node ℓ, and the translation at node ℓ is defined by the relation $\mathcal{N}_\ell \triangleq \mathcal{D}D_\ell \bowtie \mathcal{S}S_\ell$. For non-filtering nodes $\mathcal{N}_\ell$ is just the identity relation.

Similarly to the plain case, in the case of NATs we also define the *acceptance filter* of an arc and adapt it to the fact that the packets change overtime: instead of requiring the packet to be accepted at the next location, we require the acceptance of the potential translation of the packet. With this extensions, Theorem 15 can be lifted to the NAT case.

And finally, as in the plain case, we define the firewall behaviour $\mathcal{FW}$ based on the KEEP_* sets and combining the potential translations. If $\mathsf{sender}(c_i) = \ell_i, \mathsf{rcpt}(c_i) = \mathsf{sender}(c_o) = \ell_f$, and $\mathsf{rcpt}(c_o) = \ell_o$, then $\mathcal{FW}(t, c_i, c_o, p)$ is defined as $\mathcal{N}_{\ell_f}(p)$ if (i) $\mathcal{N}_{\ell_f}(p) \subseteq \mathsf{KEEP}_*(\ell_f)$ (that is, the message is accepted by ℓ_f after the NATs) and (ii) $\mathcal{N}_{\ell_f} \bowtie \mathcal{N}_{\ell_o}(p) \subseteq \mathsf{KEEP}_*(\ell_o)$ (that is, the next node is also going to accept this translated messge), and empty otherwise.

V. Semantic Based Implementation

The theory developed so far considers a very general notion of firewall $\mathcal{FW}$ whose behaviour depends on the firewall history and on the actual input and output channels. We now show how this general notion can be implemented using an extension of Mignis [1], a semantic based tool for firewall configuration in Linux systems. Mignis has a formal semantics that permits to formally prove correctness with respect to our frame semantics and, at the same time, is provided with an open-source compiler[1] that will allow us to produce working Linux firewalls, as illustrated in Section V-B. Notice that Mignis is a general firewall language and is not tailored only to Linux systems so, in principle, it is possible to generate configurations also for other firewall systems.

A. Mignis and its Semantics

Mignis [1] is a declarative specification language in which the order of rules does not matter. This makes the specification of a firewall very close to its semantics: a packet goes through (possibly translated) only if it matches a positive rule and is not explicitly denied. This allows administrators to write and

[1] https://github.com/secgroup/Mignis

inspect rules independently of the order in which they are specified. Moreover, the declarative approach makes it easy to detect possible conflicts and redundancies and to query for a subset of the specification involving specific hosts. Mignis supports Network Address Translation (NAT), i.e., it allows the translation of the source and destination addresses of a packet while it crosses the firewall, and it applies the translation consistently to all packets belonging to the same connection.

Mignis rules are defined in terms of address ranges $\mathtt{n}$. An address range $\mathtt{n}$ is a pair consisting of a set of IP addresses and a set of ports, denoted $IP(\mathtt{n})$:$port(\mathtt{n})$. Given an address $\mathtt{addr}$, we write $\mathtt{addr} \in \mathtt{n}$ to denote $port(\mathtt{addr}) \in port(\mathtt{n})$, if $port(\mathtt{addr})$ is defined, and $IP(\mathtt{addr}) \in IP(\mathtt{n})$. Notice that if $\mathtt{addr}$ does not specify a port (for example in ICMP packets) we only check if the IP address is in the range. We will use the wildcard $*$ to denote any possible address or port or address range, and ϵ to denote a special range consisting of a special address $\epsilon_{\mathtt{addr}}$ used to note void translations.

Syntax: We present a version of Mignis (that we call $\mathtt{Mignis}^+$) that extends the original one in various respects: (i) rules are localized on channels $\mathcal{CH}$ in order to allow for packet filtering that depends on the network topology; (ii) packets on established connections are not accepted by default; (iii) rules are all positive. $\mathtt{Mignis}^+$ is slightly more complex to use but strictly more expressive than the original one. Since we will generate $\mathtt{Mignis}^+$ configurations automatically we do not consider the increased complexity as a problem. The $\mathtt{Mignis}^+$ syntax follows:

$$r \quad ::= \quad \mathtt{n_s}\ [\mathtt{n_s^t}]\ @\ \mathtt{c_s} > \mathtt{n_d}\ [\mathtt{n_d^t}]\ @\ \mathtt{c_d} : \phi$$

where ϕ is a predicate that is checkable over a packet and the firewall state represented in terms of a trace, as defined in section II-A. Intuitively, this rule accepts a packet p from $\mathtt{n_s}$ to $\mathtt{n_d}$ that is received from channel $\mathtt{c_s}$ and is routed to channel $\mathtt{c_d}$ whenever $\phi(p,t)$ holds. Packet p's source and destination addresses are translated into different ones belonging to $\mathtt{n_s^t}$ and $\mathtt{n_d^t}$ in order to support NAT. When $\mathtt{n_s^t}$ and $\mathtt{n_d^t}$ are ϵ the rule leaves the addresses unchanged. When, instead, $\mathtt{n_s^t}$ and $\mathtt{n_d^t}$ are different from ϵ, they respectively correspond to source and destination NATs, and if both source and destination NATs are specified they are combined together.[2] A sequence of these firewall rules is called a *configuration*, $C ::= r; C \mid \langle\rangle$

Semantics: Mignis implements NAT by keeping track of the established connections and the relative address translations. In this paper we represent $\mathtt{Mignis}^+$ state as a trace representing previous sent and received packets with the respective channels, as defined in section II-A. Let $PK = [(\mathcal{CH} \times \mathcal{D})^* \to \mathcal{CH} \to \mathcal{CH} \to P \to \mathcal{P}(P)]$ be the domain of packet transformers. We define $[\![\cdot]\!] : C \to PK$, i.e., a function mapping a $\mathtt{Mignis}^+$ configuration C into a packet transformer, representing all the accepted packets with the corresponding translations. $[\![\cdot]\!]\, t\, c_i\, c_o\, p$ is defined inductively in Table I, where $\phi_{\mathtt{n_s},\mathtt{n_d}}(p,t) \triangleq \mathtt{sa}(p) \in \mathtt{n_s} \wedge \mathtt{da}(p) = \mathtt{n_d} \wedge \phi(p,t)$ and $p[\mathtt{sa} \mapsto \mathtt{a_s^t}, \mathtt{da} \mapsto \mathtt{a_d^t}]$ denotes packet p where $\mathtt{sa}(p)$, respectively $\mathtt{da}(p)$, is replaced by $\mathtt{a_s^t}$, respectively $\mathtt{a_d^t}$, if it is different from the void address $\epsilon_{\mathtt{addr}}$, and left unchanged otherwise.

Intuitively, the empty configuration $\langle\rangle$ corresponds to the empty set. For a configuration $\mathtt{n_s}\ [\mathtt{n_s^t}]\ @\ \mathtt{c_i} > \mathtt{n_d}\ [\mathtt{n_d^t}]\ @\ \mathtt{c_o} : \phi\ ;\ C$ we take all the packets that are received on c_i, routed on c_o and satisfy $\phi_{\mathtt{n_s},\mathtt{n_d}}(p,t)$, whose addresses are translated along non-ϵ NATs $\mathtt{n_s^t}, \mathtt{n_d^t}$, together with the packets returned by the remaining rules in C. By taking this union with the remaining rules in C we are indeed considering that there is no ordering in the rules of a $\mathtt{Mignis}^+$ configuration.

Definition 20 ($\mathtt{Mignis}^+$ firewall)**.** Given a $\mathtt{Mignis}^+$ configuration C, we let $\mathcal{FW}(t,c,c',p) \triangleq [\![C]\!]\, t\, c\, c'\, p$.

Example 21. Consider a destination NAT that translates all tcp incoming packets from interface `eth0` directed to 192.168.0.1 port 80 on interface `eth1`, into address 192.168.0.100 on the same port. In $\mathtt{Mignis}^+$ this is specified through a configuration C composed of a single rule:

$$*@\mathtt{eth0} > 192.168.0.1{:}80@\mathtt{eth1}\ [192.168.0.100{:}80] : \mathrm{tcp}$$

where we omit writing the void $[\epsilon_{\mathtt{addr}}]$ source NAT, for readability, and where tcp corresponds to a predicate that holds if and only if p is a tcp packet. We have:

$$[\![C]\!]\, t\, c_i\, c_o\, p = \{p[\mathtt{da} \mapsto 192.168.0.100{:}80]\}$$

if $\mathtt{da}(p) = 192.168.0.1{:}80, c_i = \mathtt{eth0}, c_o = \mathtt{eth1}, \mathrm{tcp}(p)$. This firewall will accept any tcp packet from `eth0` with destination 192.168.0.1:80 on `eth1` and will translate its destination to 192.168.0.100:80. For example, let p be a tcp packet with source 1.2.3.4:5656 and destination 192.168.0.1:80. We have $[\![C]\!]\, t\, \mathtt{eth0}\, \mathtt{eth1}\, p = \{p[\mathtt{da} \mapsto 192.168.0.100{:}80]\}$. Notice that the fact packet is tcp is independent of the firewall history t, so firewall semantics does not depend on t in this specific example.

B. A Tool for Firewall Localization

We have implemented a tool that given a network specification and a set of region control rules automatically localizes the filters and generates $\mathtt{Mignis}^+$ configurations for all the firewalls in the network. We have also modified the original Mignis compiler by incorporating the extensions illustrated in section V-A in order to produce the actual Linux firewall (Netfilter) configurations. The tool is implemented in Python3.

Network: We consider a network consisting of firewalls and end hosts, and we assume that each channel has at least one firewall endpoint. This ensures that all edges can filter packets.

Constraints: Given rule $\psi_B@B \to \phi@R \to \psi_E@E$, we specify constraints ψ_B, ψ_E and ϕ as Boolean expressions over variables representing the following facts:

Source and destination address whenever a packet has source or destination address of end host `h`, written `sa_h` and `da_h`, respectively;

Source and destination port whenever a packet has a source or destination port `n`, written `sp_n` and `dp_n`, respectively;

[2]Notice that square brackets are used consistently to note the translated addresses. This differs from the original Mignis notation for destination NATs which encloses in square brackets the address before translation, i.e., $\mathtt{n_d}$.

$$[\![\langle\rangle]\!]\, t\, c_i\, c_o\, p \triangleq \{\}$$

$$[\![\mathtt{n_s}\ [\mathtt{n_s^t}]\ @\ \mathtt{c_i} > \mathtt{n_d}\ [\mathtt{n_d^t}]\ @\ \mathtt{c_o} : \phi\ ;\ C]\!]\, t\, c_i\, c_o\, p \triangleq [\![C]\!]\, t\, c_i\, c_o\, p \cup \begin{cases} \{p[\mathtt{sa} \mapsto \mathtt{a_s^t}, \mathtt{da} \mapsto \mathtt{a_d^t}] \\ \quad \mid \mathtt{a_s^t} \in \mathtt{n_s^t}, \mathtt{a_d^t} \in \mathtt{n_d^t}\} & \text{if } \mathtt{c_i} = c_i, \mathtt{c_o} = c_o, \phi_{\mathtt{n_s},\mathtt{n_d}}(p,t) \\ \{\} & \text{otherwise} \end{cases}$$

TABLE I
$\texttt{Mignis}^+$ SEMANTICS.

Protocol whenever packet protocol is `p`, written `pr_p`;
Established whenever a packet belongs to an established connection, written `est`.

For example, `sp_443` & `est` requires that the source port is 443, and that packets belong to an established connection. This is a typical example of a response from a SSL web server. Notice that we use notations &, | and $\sim$ to represent Boolean AND, OR and NOT, respectively. Rules apply only to non-spoofed, non-promiscuous packets. This is automatically enforced by requiring ψ_B&`sa_B` and ψ_E&`sa_E` in place of ψ_B and ψ_E.

Localization: We compute localization as described in section IV. At the moment the prototype only supports the case without NATs described in section IV-A. We leave the extension to NATs as a future work. Constraints are represented as reduced, ordered BDD (ROBDD) [4]. We base our implementation on the Python EDA library that supports both Boolean algebra and ROBDDs.[3] The advantage of adopting ROBDD representation is that it is a canonical form and makes it very efficient to compute equivalence between Boolean expressions, which is useful to determine when the computation of Rch stabilizes. Set union and intersection used for localization in section IV-A naturally become OR and AND Boolean operators over ROBDDs.

Firewall configuration: Once we obtain $\mathcal{FW}_a(t, c_i, c_o, p)$ or $\mathcal{FW}_r(t, c_i, c_o, p)$ in the form of a Boolean expression we generate $\texttt{Mignis}^+$ configurations by instantiating the expression with the source and destination addresses of any possible end host, and by computing the solutions of the obtained boolean expression. It is worth noticing that Python EDA transparently invokes PicoSAT solver [4] to efficiently solve a Boolean expression. Solutions are then translated into constraints over ports, protocol and established state.

C. Case study

We consider the case study depicted in Figure 1 composed of three subnetworks `Sensitive`, `Trusted` and `Untrusted`, two internal firewalls `fw1` and `fw2`, and two frontier firewalls `fw3` and `fw4` connecting to the `Internet`. This represents a typical scenario where internal firewalls filter traffic among subnetworks while frontier firewalls filter traffic from/to the Internet.

In our example, `Sensitive` subnetwork contains important servers and data and is connected to the `Internet` through the

[3] http://pyeda.readthedocs.org/
[4] http://fmv.jku.at/picosat/

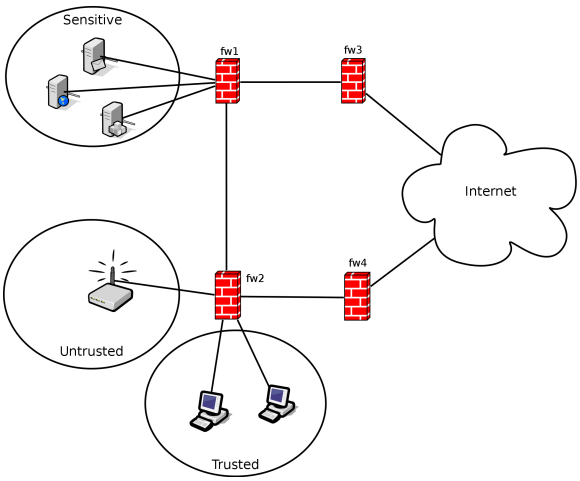


Fig. 1. A simple network with two internal and two frontier firewalls.

firewalls `fw1` and `fw3`; `Trusted` subnetwork is composed of trusted hosts that, for example, can access services hosted in the `Sensitive` subnetwork; `Untrusted` is a wifi subnetwork providing a controlled access to the `Internet` but not to services hosted in `Sensitive`. Both `Trusted` and `Untrusted` are connected to the firewall router `fw2` which in turn is connected to the other internal firewall `fw1`, and to the `Internet` through the frontier firewall `fw4`.

Security goals: We now define the security goals for the example network. As already mentioned, firewalls usually keep track of established connections so that packets belonging to the same connections are not filtered. This is particularly useful to enable bidirectional communication without necessarily opening the firewall bidirectionally to a new connection: it is enough to open the firewall in one direction and let *established* packets come back. We write `est` to note that a packet is established (cf. section V-B). While specifying rules, we proceed pair by pair so to define rules and their established counterpart (when needed) at the same time.

Hosts in the `Sensitive` and `Trusted` subnetworks should never connect to `Untrusted` and vice-versa. This is naturally expressed through two-region statements in which R corresponds to B or E (cf. Section III-A):

$$\begin{aligned} \texttt{Sensitive} &\rightarrow \textbf{false}@\texttt{Sensitive} \rightarrow \texttt{Untrusted} \\ \texttt{Untrusted} &\rightarrow \textbf{false}@\texttt{Sensitive} \rightarrow \texttt{Sensitive} \\ \texttt{Trusted} &\rightarrow \textbf{false}@\texttt{Trusted} \rightarrow \texttt{Untrusted} \\ \texttt{Untrusted} &\rightarrow \textbf{false}@\texttt{Trusted} \rightarrow \texttt{Trusted} \end{aligned}$$

Hosts in the Sensitive subnetwork should never connect to Trusted, while hosts from Trusted network can access Sensitive via ssh through fw1 without passing through the Internet as this would unnecessarily expose network connections to attacks. Notice that we filter packets from Sensitive to Trusted only if they do not belong to established ssh connections:

$$\begin{aligned}
\texttt{Trusted} &\rightarrow \quad \mathbf{dp_22}@\texttt{Sensitive} \quad \rightarrow \texttt{Sensitive}\\
\texttt{Sensitive} &\rightarrow (\mathbf{sp_22}\&\texttt{est})@\texttt{Sensitive} \rightarrow \texttt{Trusted}\\
\texttt{Trusted} &\rightarrow \quad \mathbf{false}@\texttt{Internet} \quad \rightarrow \texttt{Sensitive}\\
\texttt{Sensitive} &\rightarrow \quad \mathbf{false}@\texttt{Internet} \quad \rightarrow \texttt{Trusted}
\end{aligned}$$

Sensitive should access the Internet only via https (destination port 443), while Internet hosts should never start new connections towards Sensitive:

$$\begin{aligned}
\texttt{Sensitive} &\rightarrow \quad \mathbf{dp_443}@\texttt{Sensitive} \quad \rightarrow \texttt{Internet}\\
\texttt{Internet} &\rightarrow (\mathbf{sp_443}\&\texttt{est})@\texttt{Sensitive} \rightarrow \texttt{Sensitive}
\end{aligned}$$

Trusted has full access to the Internet and from the Internet we give access to Trusted only via ssh (port 22). Notice that full access if granted by do not specifying any region control statement but we still need to leave established packets go through:

$$\texttt{Internet} \rightarrow (\mathbf{dp\_22}|\texttt{est})@\texttt{Trusted} \rightarrow \texttt{Trusted}$$

Untrusted should access the Internet exclusively through fw3 on port 80. This is a form of traversal control that can be compiled into region control rules by taking cut $\{\texttt{fw3}, \texttt{fw4}\}$ and forbidding traversal of everything but fw3, i.e., fw4 (cf. Section III-A). In a real setting, this might be motivated by the fact fw3 is more powerful than fw4 being able to handle complex (stateful) protocols and offering logging capabilities that are useful to check what the untrusted users do. Internet should never access Untrusted:

$$\begin{aligned}
\texttt{Untrusted} &\rightarrow \quad \mathbf{dp_80}@\texttt{fw3} \quad \rightarrow \texttt{Internet}\\
\texttt{Internet} &\rightarrow (\mathbf{sp_80}\&\texttt{est})@\texttt{fw3} \rightarrow \texttt{Untrusted}\\
\texttt{Untrusted} &\rightarrow \quad \mathbf{false}@\texttt{fw4} \quad \rightarrow \texttt{Internet}\\
\texttt{Internet} &\rightarrow \quad \mathbf{false}@\texttt{fw4} \quad \rightarrow \texttt{Untrusted}
\end{aligned}$$

Localizing filtering: Table II in the Appendix reports the output of the localization tool that automatically generated the Mignis$^+$ configuration for the four firewalls according to $\mathcal{FW}_r(t, c_i, c_o, p)$. Channels/interfaces are named with prefix if_ to distinguish them from network end hosts. For example, the first group of rules for firewall fw1

```
Sensitive@if_Sensitive:22 > Trusted@if_fw2 | -m ...
Sensitive@if_Sensitive    > Internet@if_fw2:443
```

refer to interfaces if_Sensitive and if_fw2, i.e., packets coming from the the channel connecting Sensitive to fw1 and delivered over the channel from fw1 to fw2. Established requirement is translated into the low level syntax of Linux firewall:

```
-m state --state ESTABLISHED,RELATED
```

We can see that, on these two channels, firewall fw1 only allows packets from Sensitive to Trusted on established ssh connections and new https connections from Sensitive to Internet, as required by the region control rules:

$$\begin{aligned}
\texttt{Sensitive} &\rightarrow (\mathbf{sp_22}\&\texttt{est})@\texttt{Sensitive} \rightarrow \texttt{Trusted}\\
\texttt{Sensitive} &\rightarrow \quad \mathbf{dp_443}@\texttt{Sensitive} \quad \rightarrow \texttt{Internet}
\end{aligned}$$

We illustrate in detail how the following rules, permitting access from Unstrusted to Internet only on port 80 through fw3, are localized in the firewalls:

$$\begin{aligned}
\texttt{Untrusted} &\rightarrow \quad \mathbf{dp_80}@\texttt{fw3} \quad \rightarrow \texttt{Internet}\\
\texttt{Internet} &\rightarrow (\mathbf{sp_80}\&\texttt{est})@\texttt{fw3} \rightarrow \texttt{Untrusted}\\
\texttt{Untrusted} &\rightarrow \quad \mathbf{false}@\texttt{fw4} \quad \rightarrow \texttt{Internet}\\
\texttt{Internet} &\rightarrow \quad \mathbf{false}@\texttt{fw4} \quad \rightarrow \texttt{Untrusted}
\end{aligned}$$

The relevant rules are:

```
FIREWALL fw1
Untrusted@if_fw2 > Internet@if_fw3:80
Internet@if_fw2:80 > Untrusted@if_fw3       | -m ...
Untrusted@if_fw3 > Internet@if_fw2:80
Internet@if_fw3:80 > Untrusted@if_fw2       | -m ...

FIREWALL fw2
Untrusted@if_Untrusted > Internet@if_fw1:80
Internet@if_fw1:80 > Untrusted@if_Untrusted | -m ...

FIREWALL fw3
Internet@if_Internet:80 > Untrusted@if_fw1  | -m ...
Untrusted@if_fw1 > Internet@if_Internet:80
```

Firewall fw1 allows for bidirectional traffic between fw2 and fw3 on the required ports. Notice that packets from Untrusted to Internet from fw3 to fw2 would necessarily result in a cyclic routing which would be prevented by the actual routers. However, allowing this traffic is not contradicting the security goal. Firewalls fw2 and fw3 enable traffic towards fw1. Packets from Untrusted to Internet are dropped in fw4 (which contains no rule between those two end hosts), and on the link from fw2 to fw4, as required.

VI. Conclusions

In this paper we have provided a way to specify security goals for how packets traverse the network together with a way to distribute filtering functionality to different nodes in the network. We have proved that the obtained filtering implements the security constraints while providing maximal service functionality. We have finally implemented and verified our results using a tool that automatically localizes the filters and generates configurations for all the firewalls in the network.

As a future work, from a theoretical point of view we plan to give an enforcement of the spoofing goals (that consider only trajectories with spoofing at creation), and promiscuous delivery goals (i.e., trajectories with promiscuous delivery). From a practical point of view we plan to extend our tool for localising the filters also in the case of NATs.

REFERENCES

[1] P. Adao, C. Bozzato, R. Focardi G. Dei Rossi, and F.L. Luccio. Mignis: A semantic based tool for firewall configuration. In *IEEE 27th Computer Security Foundations Symposium (CSF 2014), Vienna, Austria*, pages 351–365. IEEE CS Press, July 2014.

[2] E. Al-Shaer, A. El-Atawy, and T. Samak. Automated Pseudo-Live Testing of Firewall Configuration Enforcement. *IEEE Journal on selected areas in communication*, 27(3):302–314, 2009.

[3] C. J. Anderson, N. Foster, A. Guha, J.-B. Jeannin, D. Kozen, C. Schlesinger, and D. Walker. NetKAT: Semantic foundations for networks. In *Proc. of the 41st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 2014)*. ACM, 2014.

[4] Randal E. Bryant. Graph-based algorithms for boolean function manipulation. *IEEE Trans. Comput.*, 35(8):677–691, August 1986.

[5] Frenetic, a family of network programming languages. http://www.frenetic-lang.org/, 2013.

[6] J.D. Guttman and A.L. Herzog. Rigorous automated network security management. *International Journal for Information Security*, 5(1–2):29–48, 2005.

[7] J.D Guttman and P.D. Rowe. A cut principle for information flow. In *IEEE 28th Computer Security Foundations Symposium (CSF 2015), Verona, Italy*, pages 107–121. IEEE CS Press, July 2015.

[8] Ahmed Khurshid, Wenxuan Zhou, Matthew Caesar, and PB Godfrey. Veriflow: verifying network-wide invariants in real time. *ACM SIGCOMM Computer Communication Review*, 42(4):467–472, 2012.

[9] T. Nelson, C. Barratt, D.J. Dougherty, K. Fisler, and S. Krishnamurthi. The margrave tool for firewall analysis. In *Proceedings of the 24th International Conference on Large Installation System Administration (LISA'10)*, pages 1–8, Berkeley, CA, USA, 2010. USENIX Association.

[10] J. Walsh. Icsa labs firewall testing: An in depth analysis. http://bandwidthco.com/whitepapers/netforensics/penetration/Firewall%20Testing.pdf, 2004.

[11] B. Zhang, E. Al-Shaer, R. Jagadeesan, J. Riely, and C. Pitcher. Specifications of a high-level conflict-free firewall policy language for multi-domain networks. In *Proc. of ACM Symposium on Access Control Models and Technologies (SACMAT 2007)*. ACM, 2007.

APPENDIX

Table II reports the output of the localization tool that automatically generated the `Mignis`$^{+}$ configuration for the four firewalls.

```
FIREWALL fw1

   Sensitive@if_Sensitive   : 22         >      Trusted@if_fw2                | -m state --state ESTABLISHED,RELATED
   Sensitive@if_Sensitive               >     Internet@if_fw2         : 443

   Sensitive@if_Sensitive   : 22         >      Trusted@if_fw3                | -m state --state ESTABLISHED,RELATED
   Sensitive@if_Sensitive               >     Internet@if_fw3         : 443

     Trusted@if_fw2                     >    Sensitive@if_Sensitive   : 22
    Internet@if_fw2         : 443       >    Sensitive@if_Sensitive            | -m state --state ESTABLISHED,RELATED

   Untrusted@if_fw2                     >     Internet@if_fw3         : 80
     Trusted@if_fw2                     >     Internet@if_fw3
    Internet@if_fw2         : 80        >    Untrusted@if_fw3                  | -m state --state ESTABLISHED,RELATED
    Internet@if_fw2                     >      Trusted@if_fw3         : 22
    Internet@if_fw2                     >      Trusted@if_fw3                  | -m state --state ESTABLISHED,RELATED

     Trusted@if_fw3                     >    Sensitive@if_Sensitive   : 22
    Internet@if_fw3         : 443       >    Sensitive@if_Sensitive            | -m state --state ESTABLISHED,RELATED

   Untrusted@if_fw3                     >     Internet@if_fw2         : 80
     Trusted@if_fw3                     >     Internet@if_fw2
    Internet@if_fw3         : 80        >    Untrusted@if_fw2                  | -m state --state ESTABLISHED,RELATED
    Internet@if_fw3                     >      Trusted@if_fw2         : 22
    Internet@if_fw3                     >      Trusted@if_fw2                  | -m state --state ESTABLISHED,RELATED


FIREWALL fw2

     Trusted@if_Trusted                 >    Sensitive@if_fw1         : 22
     Trusted@if_Trusted                 >     Internet@if_fw1

     Trusted@if_Trusted                 >    Sensitive@if_fw4         : 22
     Trusted@if_Trusted                 >     Internet@if_fw4

   Untrusted@if_Untrusted               >     Internet@if_fw1         : 80

   Sensitive@if_fw1         : 22        >      Trusted@if_Trusted             | -m state --state ESTABLISHED,RELATED
    Internet@if_fw1                     >      Trusted@if_Trusted      : 22
    Internet@if_fw1                     >      Trusted@if_Trusted             | -m state --state ESTABLISHED,RELATED

    Internet@if_fw1         : 80        >    Untrusted@if_Untrusted           | -m state --state ESTABLISHED,RELATED

   Sensitive@if_fw1                     >     Internet@if_fw4         : 443
    Internet@if_fw1         : 443       >    Sensitive@if_fw4                  | -m state --state ESTABLISHED,RELATED

   Sensitive@if_fw4         : 22        >      Trusted@if_Trusted             | -m state --state ESTABLISHED,RELATED
    Internet@if_fw4                     >      Trusted@if_Trusted      : 22
    Internet@if_fw4                     >      Trusted@if_Trusted             | -m state --state ESTABLISHED,RELATED

   Sensitive@if_fw4                     >     Internet@if_fw1         : 443
    Internet@if_fw4         : 443       >    Sensitive@if_fw1                  | -m state --state ESTABLISHED,RELATED


FIREWALL fw3

    Internet@if_Internet    : 443       >    Sensitive@if_fw1                  | -m state --state ESTABLISHED,RELATED
    Internet@if_Internet    : 80        >    Untrusted@if_fw1                  | -m state --state ESTABLISHED,RELATED
    Internet@if_Internet                >      Trusted@if_fw1         : 22
    Internet@if_Internet                >      Trusted@if_fw1                  | -m state --state ESTABLISHED,RELATED

   Sensitive@if_fw1                     >     Internet@if_Internet    : 443
   Untrusted@if_fw1                     >     Internet@if_Internet    : 80
     Trusted@if_fw1                     >     Internet@if_Internet


FIREWALL fw4

    Internet@if_Internet    : 443       >    Sensitive@if_fw2                  | -m state --state ESTABLISHED,RELATED
    Internet@if_Internet                >      Trusted@if_fw2         : 22
    Internet@if_Internet                >      Trusted@if_fw2                  | -m state --state ESTABLISHED,RELATED

   Sensitive@if_fw2                     >     Internet@if_Internet    : 443
     Trusted@if_fw2                     >     Internet@if_Internet
```

TABLE II

Mignis^{+} RULES AUTOMATICALLY GENERATED FOR THE FOUR FIREWALLS OF THE EXAMPLE NETWORK.