Read or listen to this article online

Scan the QR code to open this article on XO.PL

Article source:

https://xo.pl/it-made-fun-sec-firewall

IT SECURITY

Firewalls: the border crossing of the Republic of Packets

In the Republic of Packets, every citizen had an address, every service had a doorway, and the border had a barrier. Things had worked fairly well for years, until the Manager was appointed Minister for Traffic Improvement. On his first morning, he arrived in a government car, saw a queue of lorries and announced a reform that nearly finished off the entire republic before breakfast. 🛂🚧🤣

— GREGORY! — he shouted at the border guard commander. — WHY ARE THOSE VEHICLES WAITING?!

— Because we check where they're going and whether they're allowed through.

— BUT THEY WANT TO GO THROUGH!

— That's why we have a barrier. If they didn't, we wouldn't need one.

Agnes, head of border records, looked at the pile of ministerial decrees.

— Minister, perhaps you should read the rules first.

— RULE NUMBER ONE: NO QUEUES!

Gregory closed his eyes. The Republic of Packets was barely awake. Trouble was already at work.

A border that cannot read minds

Gregory showed the Minister a map. On one side were offices, servers and citizens. On the other was a huge world full of ordinary visitors, clients, couriers and, occasionally, unwelcome guests.

— A firewall is like border control. It evaluates traffic against configured rules and can permit, drop or reject it. Real firewalls examine information such as IP addresses, protocols, ports, traffic direction and, when supported, connection state.

— SO IT CAN TELL WHO IS HONEST?

— No. An ordinary firewall doesn't read minds, automatically recognise every virus or guess what someone intends to do.

— BUT IT'S AT THE BORDER!

— A customs officer can inspect a lorry's papers. That doesn't reveal whether its driver will cheat his grandmother tomorrow.

Agnes wrote in the minutes: “Firewall is not a fortune-teller.”

— KEEP THAT OUT OF THE COUNTRY'S ADVERTISING! — the Minister protested.

The Grand Opening of Everything

The Minister climbed onto a crate of oranges and issued his first order.

— RAISE EVERY BARRIER! LET THE ECONOMY BREATHE!

Gregory requested the order in writing. Agnes requested a signature. The Minister signed three copies, accidentally titling one “Lunch Menu.”

The barriers lifted. Deliveries, customers and a school trip rolled into the country. Behind them came a lorry labelled “FREE INSPECTION OF EVERY DOOR.” Its driver stopped at every building and tried the handles.

— WHAT IS HE DOING? — demanded the Minister.

— Checking which services respond. That resembles port scanning. Scanning isn't the same as a successful intrusion, but exposing every internal service to the entire Internet is hardly sensible.

A van behind the lorry demanded access to the accounting database.

— Does he have authorisation? — Agnes asked.

— Nobody asked, what with the barrier up — the driver replied.

— MINISTER, THIS IS WHY WE NEED RULES! — Gregory exclaimed.

— THEN WE'LL CLOSE EVERYTHING! — the Minister shouted. — THAT WILL BE SAFE!

Agnes didn't even have time to roll her eyes.

The Grand Closing of Everything

At 9:17 sharp, every barrier slammed shut. Medical supplies for the hospital, documents for the council, a visitor to the public website and even a reply to a request sent five seconds earlier were all stopped.

— PERFECT! — declared the Minister. — NOBODY UNAUTHORISED GETS THROUGH!

— Nobody authorised gets through either — Agnes pointed out.

— A MINOR DETAIL!

A mail courier was stranded at the border.

— I've got messages for your citizens!

— ENTRY FORBIDDEN! — roared the ministerial loudspeaker.

— But we asked for that mail! — Agnes shouted back.

— SECURITY FIRST!

Gregory took the Minister up a hill overlooking the motionless traffic.

— A firewall that blocks necessary services isn't protecting a functioning system. It's paralysing it. Security should make normal, safe work possible, not turn a network into a museum of failed connections.

— AT LEAST NOBODY'S ATTACKING US NOW!

— Nobody can issue an invoice for your salary either.

— AGNES! RESTORE ACCOUNTING IMMEDIATELY!

Rules, not ministerial moods

Agnes opened a fresh ledger. Each rule described which traffic should pass and which should not. Gregory drew three columns: from where, to where, and for what purpose.

— We allow residents to reach the services they need, publish our public website for visitors and keep the internal accounting database off the open Internet, for example.

— WHAT DOCUMENTS WILL TRAVELLERS SHOW?

— In practice, firewalls may examine source and destination IP addresses, protocols, source and destination ports, interfaces and connection state. The exact capabilities depend on the equipment.

— So IP is a surname?

— In this analogy it's closer to a starting or destination address. A port identifies a service endpoint on a machine. But a port number alone doesn't prove which application actually uses it.

Agnes stamped the rulebook: “Permit justified traffic under a considered policy.”

— Default deny can make sense where the necessary services are well understood. It's often a good starting point for a company's network boundary. But it doesn't mean blindly disabling everything every employee needs.

— WHAT ABOUT MY “EVERYTHING ALLOWED” POLICY?

— We're replacing it with an actual procedure.

— BUREAUCRACY IS SO CRUEL!

The order of the stamps matters

The Minister decided to help Agnes. At the top of the rulebook, he wrote “LET EVERYONE IN,” then added fifteen specific prohibitions underneath.

— THERE! A COMPLETE LIST!

— Not on a firewall that evaluates rules in order and stops at the first matching one — Gregory explained. — On such a system, those later restrictions might never be reached.

— SO THE ORDER MATTERS?

— On many firewalls, yes. Different platforms use different processing models, so you need to understand the actual device. Overly broad rules can shadow specific ones.

Agnes crossed out the ministerial addition.

— You can write your wishes in a separate notebook.

— WHO WILL READ IT?

— Nobody has requested that privilege yet.

The courier with a reply and no invitation

A small car arrived at the barrier. Its driver carried a stamp marked “REPLY.”

— I'm going to Agnes! She sent the request!

— SHOW YOUR PERMIT! — the young guard demanded.

— I don't have one, but I have a case number!

Gregory opened the connection ledger.

— This is where a stateful firewall and connection tracking, or conntrack, are useful. If the firewall sees an allowed outgoing flow, it can recognise matching return traffic without opening a broad incoming rule to the whole world.

— What if we had no ledger? — Agnes asked.

— A stateless filter evaluates packets without tracking that connection context. Traffic must then be permitted in the appropriate directions explicitly. Tracking differs between protocols; not everything behaves like one simple conversation.

The Minister peered into the ledger.

— SO ANYBODY CAN FOLLOW SOMEONE WHO LEFT THE COUNTRY?

— No. Return traffic has to match the tracked flow and the firewall's policy. Painting “REPLY” on a bonnet doesn't make it legitimate.

— SHAME. I'VE ORDERED FIVE THOUSAND REPLY STAMPS.

Three routes: to the guardhouse, through it, and from it

Agnes unfolded a map with three arrows.

— A packet addressed to the firewall device itself isn't the same as one merely passing through it. And traffic generated by the router itself is different again.

— WHY DOES THAT MATTER?

— In the Linux model administrators know, the relevant chains include INPUT, FORWARD and OUTPUT. INPUT handles local delivery, FORWARD covers transit and OUTPUT deals with locally generated packets. The precise handling depends on the stack and its configuration.

— So locking the guardhouse door doesn't necessarily close the motorway behind it?

— Exactly. Protecting the router and filtering transit traffic aren't the same task.

The Minister thought hard.

— WHAT IF I LOCK ALL THREE?

— Then it's 9:17 all over again — Agnes replied.

The Address Translation Office isn't border police

Beside the crossing stood an office where cars leaving a private district received the republic's public address on their paperwork. The staff recorded how to deliver the replies to the right residents.

— GENIUS! — shouted the Minister. — THE WORLD'S BEST FIREWALL!

— That's NAT, or Network Address Translation — Gregory corrected him. — NAT changes address information and often port numbers. It can work together with connection tracking and may make certain unsolicited incoming connections harder, but NAT itself is not a firewall security policy.

— So changing number plates doesn't mean the driver passed a security inspection?

— Precisely. Address translation and traffic filtering are separate functions, even if one router performs both.

— BUT THE NEW PLATES LOOK MUCH MORE OFFICIAL!

— You could buy a customs officer's hat too. It still wouldn't make you a firewall.

Trust zones: not everyone gets a key to the treasury

That afternoon, a vehicle marked “GUEST WI-FI” arrived and asked for directions straight to the accounting records vault.

— BUT THEY'RE ALREADY INSIDE OUR COUNTRY! — the Minister objected.

— So what? — Agnes asked. — Restaurant guests don't get the keys to the safe.

— It's often useful to divide networks into security zones — Gregory explained. — Public servers, administration systems, staff devices and guest Wi-Fi needn't share the same access rights. Firewalls can control traffic between those zones, not just at the Internet edge.

— SO EVEN INTERNAL TRAFFIC MAY NEED RESTRICTIONS?

— Yes. One compromised device shouldn't automatically open the entire organisation.

— EVERY EMPLOYEE SHALL GET A SEPARATE COUNTRY! — decreed the Minister.

— Let's start with sensible VLANs and inter-zone policies — Gregory replied. — Our maps are complicated enough.

The border log, or “why is nothing working?”

At 2:26 p.m., an office called.

— Our network printer isn't working!

— IT MIGHT BE AN ATTACK! CLOSE THE BORDER! — the Minister suggested.

— Let's check the logs first — said Gregory.

Agnes opened the journal: time, source, destination, protocol, port and verdict. A newly introduced rule had blocked the printer's required traffic.

— So the problem is our own rulebook, not a hacker?

— This time. Logs, rule counters, testing and carefully scoped exceptions help diagnose problems. But logging every packet indiscriminately can overwhelm storage and bury important events in noise.

— I'LL LOG EVERYTHING! EVEN THE PIGEONS!

— That's precisely what I just told you not to do.

— THEN HOW WILL WE KNOW WHO'S FLYING?!

They restored the necessary traffic. The printer produced thirty-seven test sheets. The Minister kept every page as evidence of his reform's success.

Customs inspectors aren't fortune-tellers either

A new officer arrived at the crossing. Unlike the others, he could sometimes inspect more of the cargo instead of simply checking vehicle numbers.

— A better firewall? — Agnes asked.

— Some firewalls support application filtering, deeper traffic inspection, IDS or IPS. Those functions can examine more than addresses and ports, and detect certain attack patterns. But visibility depends on protocols, encryption, configuration and available resources.

— SO WE DON'T NEED ANY OTHER SECURITY NOW?

— We do. IDS mainly detects and alerts; IPS may block matching traffic. Neither guarantees detection of every threat. Updates, access controls, backups and careful users still matter.

— WHAT ABOUT HIRING A FORTUNE-TELLER? — the Minister asked.

— If she can read firewall logs, I'll consider the application — Gregory said.

The most dangerous permit

Near the end of the shift, a citizen crossed the border legitimately. He had valid papers, an allowed destination and permission to contact an external service. Once there, a stranger convinced him that security required him to reveal his password and approve an unexpected login.

— BUT HE PASSED OUR BORDER CHECK! — the Minister protested.

— Yes. His connection was allowed. A firewall couldn't know that he was about to fall for **phishing** — Gregory replied.

— THEN WHY HAVE A BARRIER AT ALL?!

— To restrict unwanted traffic and make certain attacks harder. But a firewall can't replace human judgement, system updates or **strong passwords and MFA**. Allowed traffic can still carry danger, and legitimate users can make mistakes.

Agnes put down the report.

— So there is no magic border that protects us from every foolish decision?

— If there were — Gregory sighed — we'd start with the Minister's office.

— I HEARD THAT! — came a voice through the door.

— That was the idea.

A sensible border and a living republic

The next morning, the queues had gone. Not because everything was wide open, but because the guards had sensible rules, the services had been tested and accidental blocks had been fixed. Couriers were moving, citizens were online and unwanted traffic still stopped at the barrier.

The Minister called a press conference.

— I DECLARE OUR BORDER PERFECT! NOTHING BAD WILL EVER HAPPEN AGAIN!

— No — Agnes and Gregory said together.

— THEN WHAT SHOULD I DECLARE?!

— That the firewall supports the republic's needs, rules are documented and tested, and incidents are investigated. And no device replaces common sense.

— COULD WE AT LEAST CLOSE THE BORDER FOR THE WEEKEND?

— No. The hospital still needs supplies and people still need the Internet.

— THEN OPEN EVERY GATE JUST ON FRIDAYS!

Agnes handed him a document.

— WHAT'S THIS?

— The rulebook. The one piece of paper you are not allowed to turn into an aeroplane.

A good firewall doesn't let everyone in, but it doesn't stop life either. It permits justified traffic under considered rules, makes troubleshooting possible and provides one layer of defence. Too permissive leaves doors needlessly open. Too restrictive can break the services it's meant to protect. And no barrier offers a 100% guarantee against users making foolish decisions.

The Republic of Packets Ministry of Traffic Improvement reports: barriers work, couriers are back on the road, connection tracking makes sense again, and Agnes has located the invoices for three failed border reforms. The Minister has lost his right to issue decrees through a loudspeaker. In retaliation, he attempted to open

port 65536. Border Control informed him that no such port exists. 🛂🚧🤣❤️