endian

Secure everyThing

Endian Security Administrator Training

Module :: Firewall

Overview

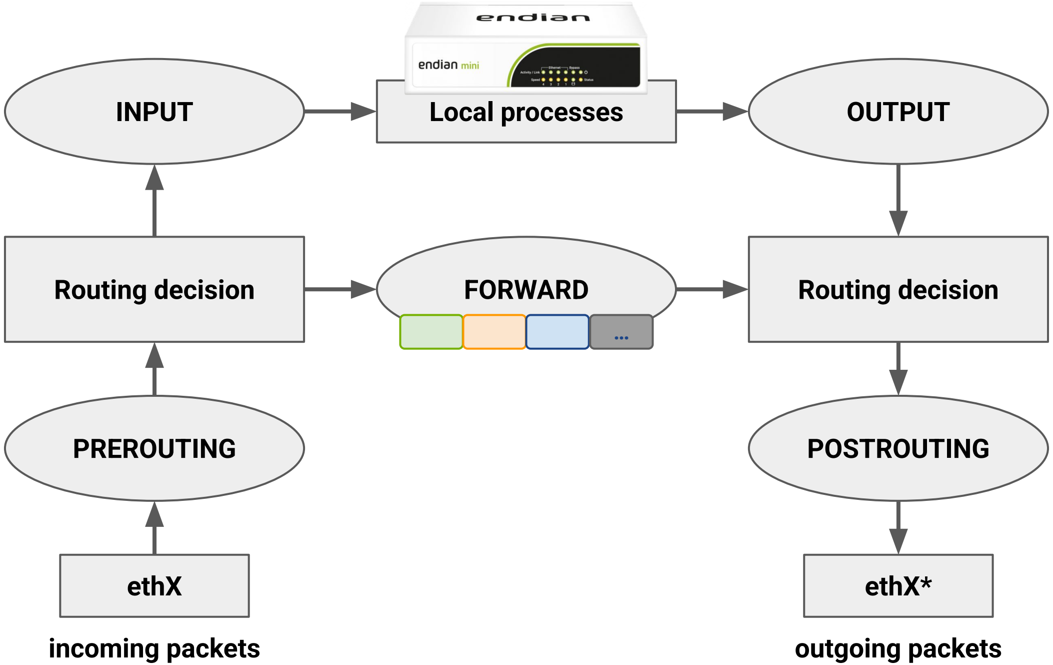
- Firewall Overview
- DNAT, SNAT, & Routed Traffic
- Outgoing Firewall

- Inter-Zone Firewall
- VPN Firewall
- System Access Firewall

endian
Secure everyThing

Module
Firewall

Netfilter main chain flow

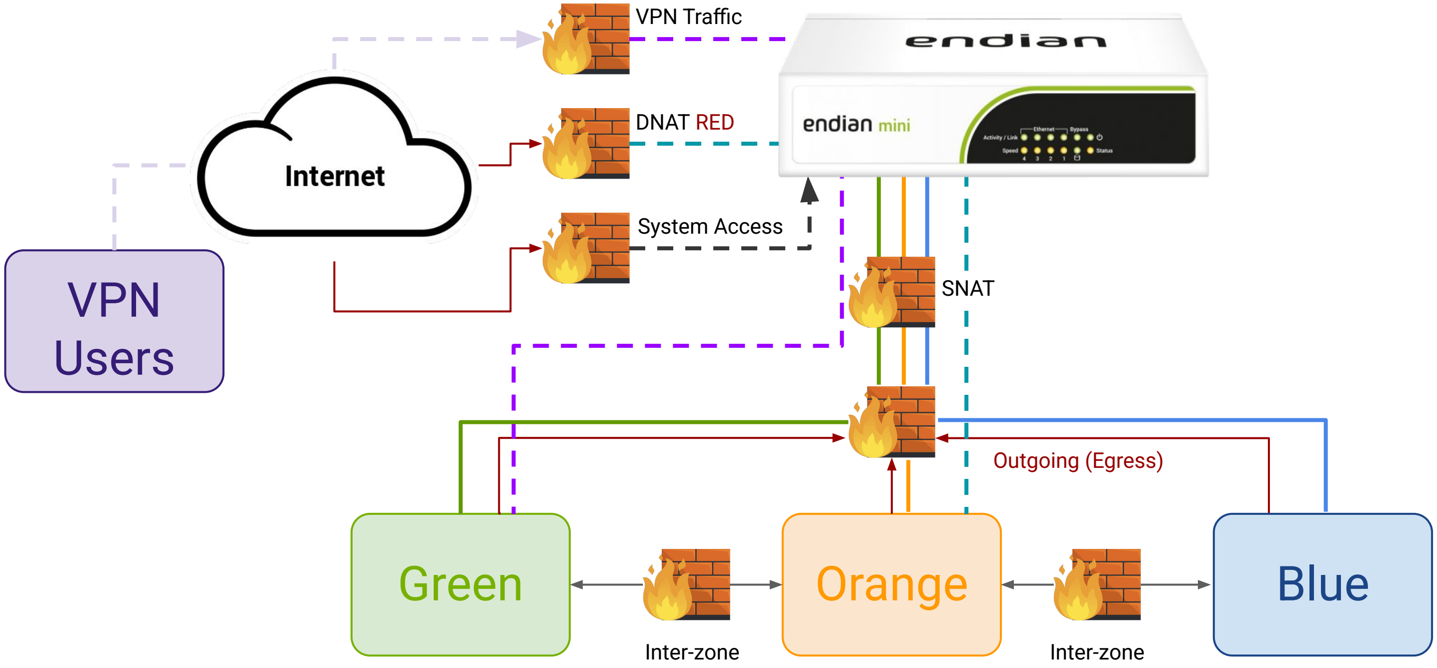


* NOTE: traffic exiting the system might be routed through a different NIC that the incoming one

endian
Secure everyThing

Module
Firewall

Endian Firewall Overview



endian
Secure everyThing

Module
Firewall

Firewall Overview

The Endian UTM appliance provides multiple predefined firewall components which you can configure uniquely to suit your network requirements. By default, each component is set to provide the highest levels of security (deny) to provide maximum protection against internal and external threats.

Firewall Component	Description	Defaults
DNAT / Port FW	Enable outside access to internal services	No inbound ports opened
Outgoing (Egress)	Enable outbound communications from internal zones (networks) to outside networks	Common set of ports opened (Web, Email, DNS, etc.)
Inter-Zone	Enable communications between the zones	Default network zone security
VPN	Enable firewall rules for VPN clients / users	Disabled by default
System Access	Enable access to Endian system (HTTPS, SSH, etc.)	No ports open from Internet

Firewall Overview - Rule Order

For any of the Firewall components (DNAT, SNAT, Outgoing, etc.) it's important to understand that the order of the rules matter! Each rule is processed in order until a successful match is found or until it reaches the end (*no match*) and the request is denied (implicit DROP policy). For this reason it's recommended to build rules from more specific to less specific (i.e. generic). This will prevent a generic rule from superseding one that was more specific and applicable.

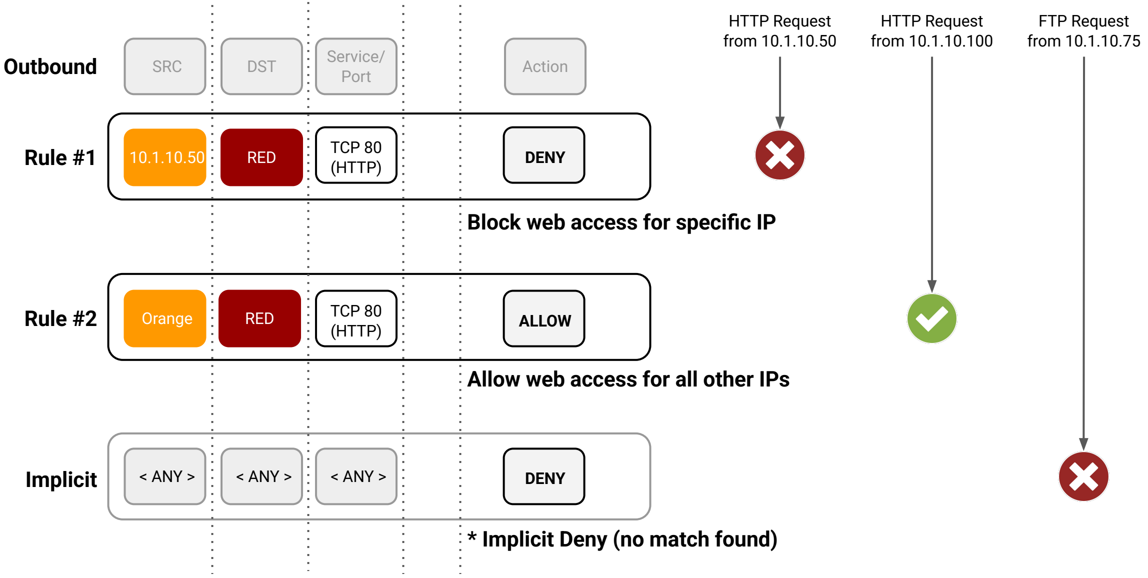
Golden rules:

- Firewall disabled: **all** traffic passes unconditionally
- Firewall enabled: what's not explicitly allowed is **DROPPED**

endian
Secure everyThing

Module
Firewall

Firewall Overview - Diagram 1



Outbound	SRC	DST	Service/ Port	Action
Rule #1	10.1.10.50	RED	TCP 80 (HTTP)	DENY
Rule #2	Orange	RED	TCP 80 (HTTP)	ALLOW
Implicit	< ANY >	< ANY >	< ANY >	DENY

Block web access for specific IP

Allow web access for all other IPs

*** Implicit Deny (no match found)**

HTTP Request from 10.1.10.50 ✗
HTTP Request from 10.1.10.100 ✓
FTP Request from 10.1.10.75 ✗

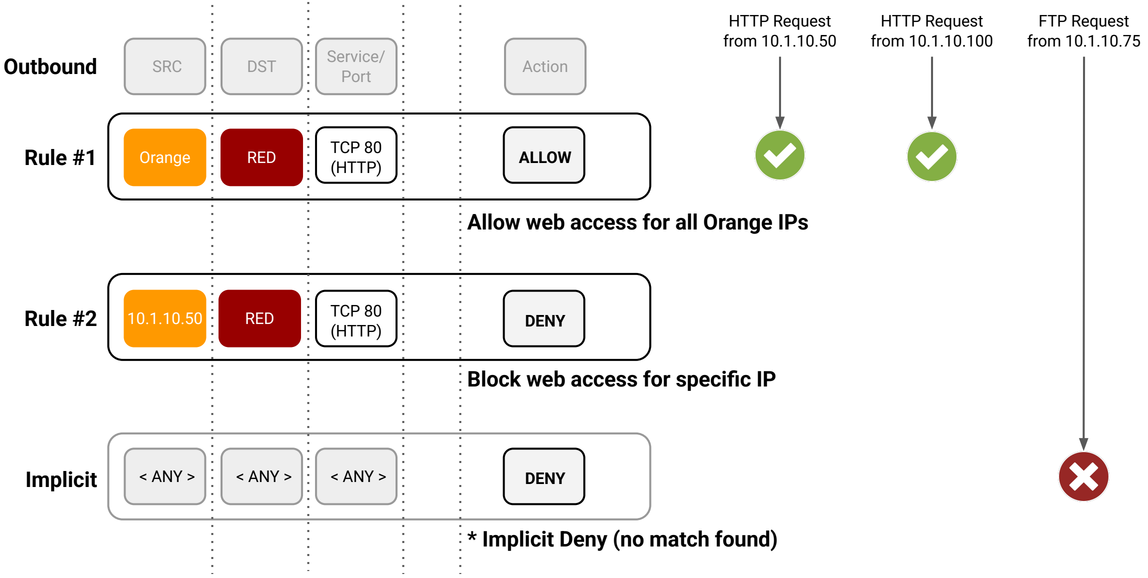
***Note:** The default system rule for any traffic not explicitly defined is for that traffic to be blocked*

endian

Secure everyThing

Module Firewall

Firewall Overview - Diagram 2



Outbound	SRC	DST	Service/ Port	Action
Rule #1	Orange	RED	TCP 80 (HTTP)	ALLOW
Rule #2	10.1.10.50	RED	TCP 80 (HTTP)	DENY
Implicit	< ANY >	< ANY >	< ANY >	DENY

Allow web access for all Orange IPs

Block web access for specific IP

* Implicit Deny (no match found)

HTTP Request from 10.1.10.50 ✓

HTTP Request from 10.1.10.100 ✓

FTP Request from 10.1.10.75 ✗

***Note:** The default system rule for any traffic not explicitly defined is for that traffic to be blocked*

Firewall Deny vs Reject

There are two different ways to implement a block rule when creating firewall rules (1) REJECT or (2) DENY/DROP

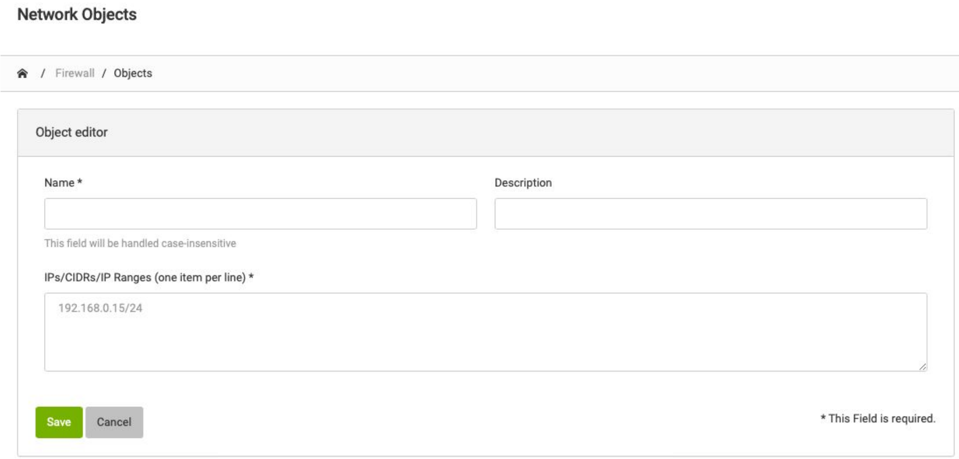
1. **REJECT**: This will send an *ICMP Port Unreachable* packet for every connection requested or packet received
2. **DENY/DROP**: This means the packet is discarded completely and no packet is sent back to the requesting machine

endian
Secure everyThing

Module
Firewall

NEW Network Objects

In many environments, the networks, IPs and network ranges are something that are well defined and thus can be reused throughout the various firewall rulesets. Endian now supports creating network objects which contain a defined list of networks, IPs, or ranges which can then be used anywhere throughout most of the firewall.



Network Objects

/ Firewall / Objects

Object editor

Name *

This field will be handled case-insensitive

Description

IPs/CIDRs/IP Ranges (one item per line) *

192.168.0.15/24

Save Cancel

* This Field is required.

Destination NAT (DNAT)

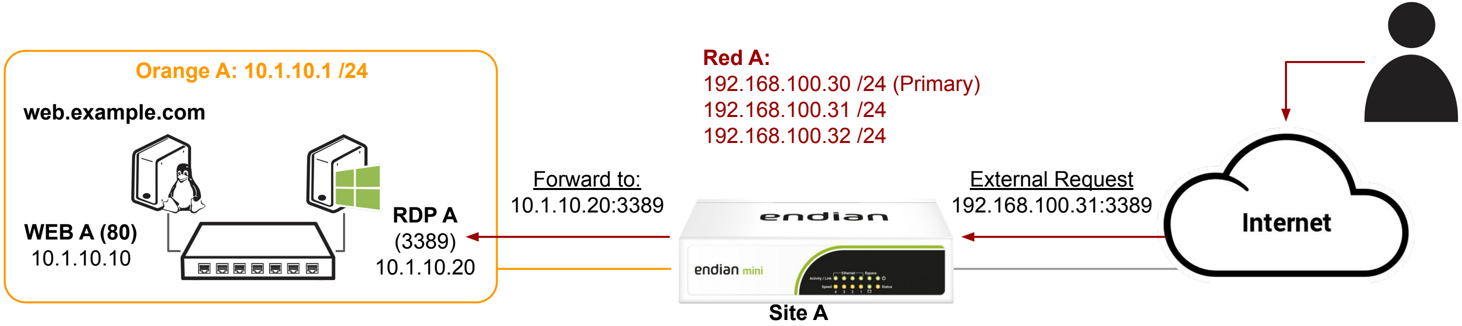
The Destination NAT provides port forwarding capability to enable access to internal resources from an external network (i.e. Internet). The most common use of this is to provision direct Internet access to internal resources (e.g. web server, file server, etc.) of the Endian. The reason Endian can do this is because typically it's deployed as the gateway appliance between the Internet and the internal, protected resources.

endian

Secure everyThing

Destination NAT (DNAT / Port Forward)

Module Firewall

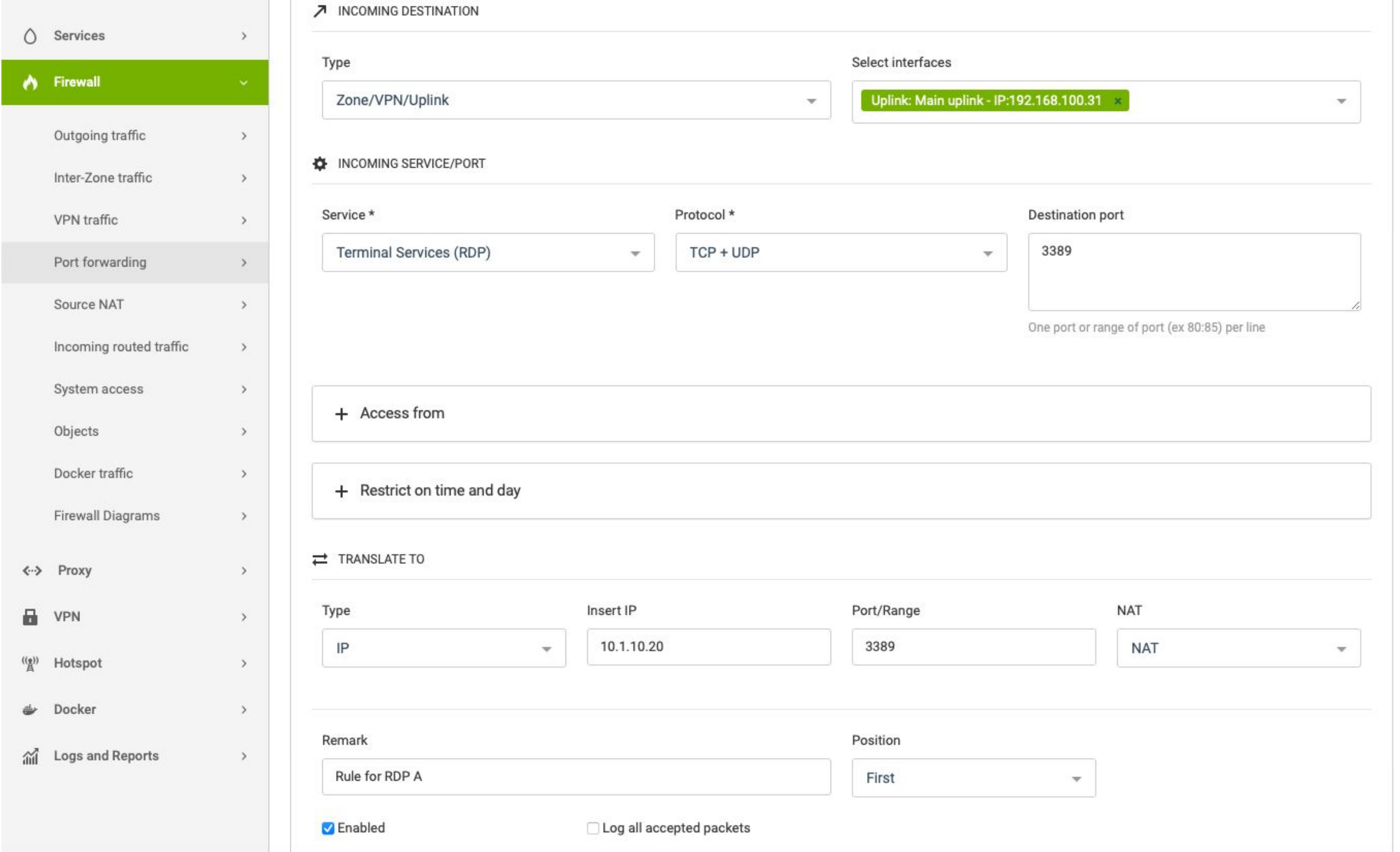


Example: Let’s use a sample network and add a DNAT rule that provides RDP (TCP/3389) access to an internal server (10.1.10.20) using an existing external IP address (192.168.100.31).

endian

Secure everyThing

Module
Firewall



INCOMING DESTINATION

Type: Zone/VPN/Uplink

Select interfaces: Uplink: Main uplink - IP:192.168.100.31 ×

INCOMING SERVICE/PORT

Service *: Terminal Services (RDP)

Protocol *: TCP + UDP

Destination port: 3389

One port or range of port (ex 80:85) per line

+ Access from

+ Restrict on time and day

TRANSLATE TO

Type: IP

Insert IP: 10.1.10.20

Port/Range: 3389

NAT: NAT

Remark: Rule for RDP A

Position: First

☑ Enabled

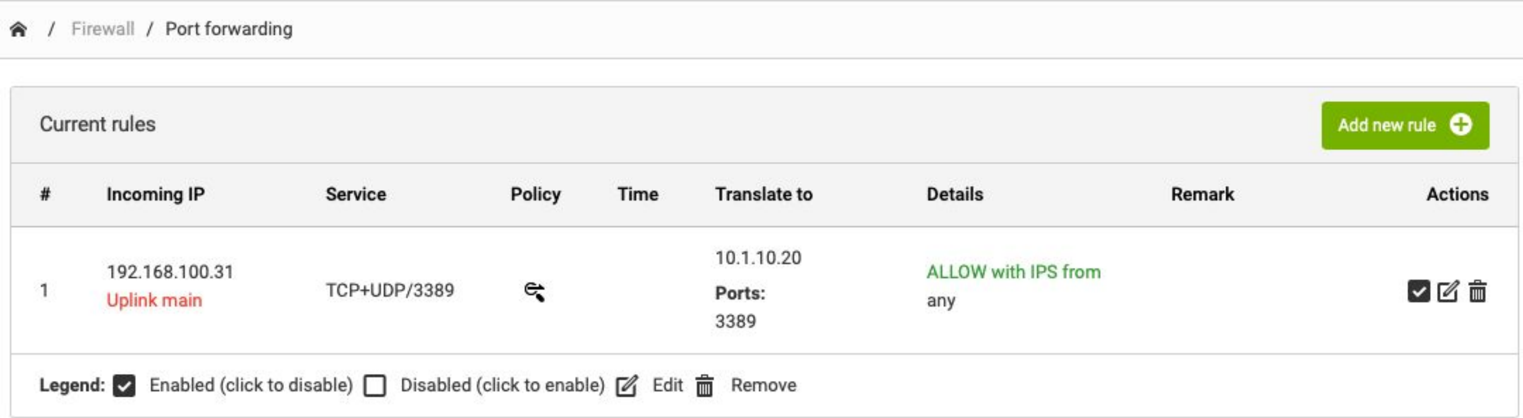
□ Log all accepted packets

Destination NAT - Example

endian

Secure everyThing

Module Firewall



#	Incoming IP	Service	Policy	Time	Translate to	Details	Remark	Actions
1	192.168.100.31 Uplink main	TCP+UDP/3389			10.1.10.20 **Ports:** 3389	ALLOW with IPS from any		☑ ✎ 🗑

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit 🗑 Remove

Destination NAT - Example

DNAT Tips & Tricks

When creating a DNAT rule, you can toggle advanced features to get additional filtering options. This includes things like GeoIP filtering, Time/Day restrictions, 1:1 Subnet mappings, basic load balancing, and advanced rule security to limit access to rules by source.

Note: By default the DNAT GUI is displayed in “simple mode” with advanced features collapsed to streamline and simplify the user experience.

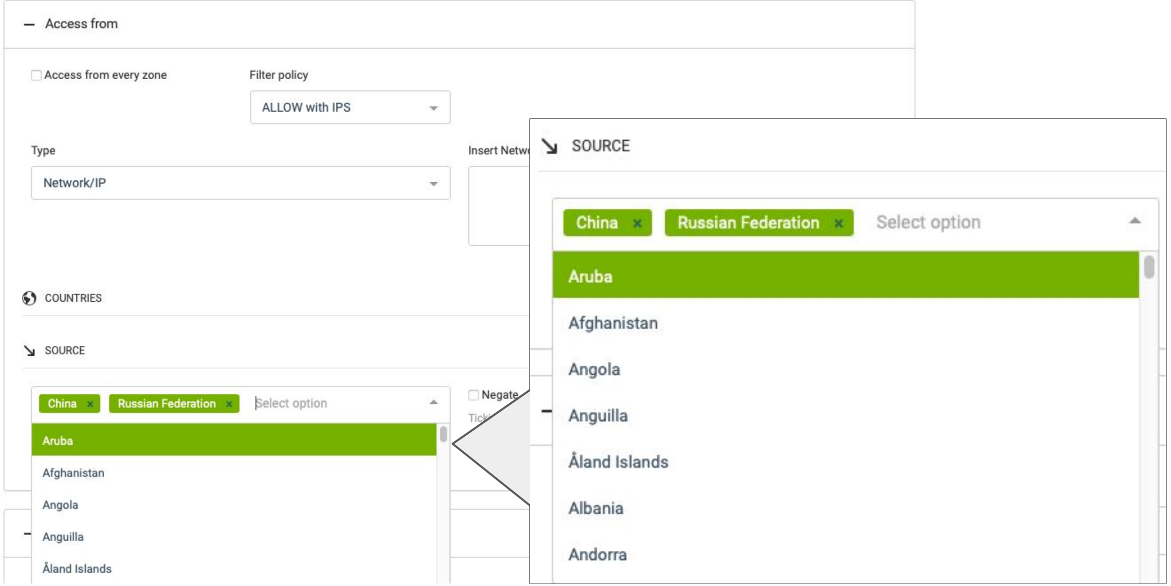
endian
Secure everyThing

Module
Firewall

DNAT Tips & Tricks

NEW GeoIP Filtering

You can create a DNAT rule that can be restricted by country or countries (based on GeoIP information). This can be done in addition to all other DNAT security restrictions including network/IP address source restrictions.



– Access from

☐ Access from every zone

Filter policy: ALLOW with IPS

Type: Network/IP

Insert Netw

COUNTRIES

SOURCE

China × Russian Federation × Select option

Aruba
Afghanistan
Angola
Anguilla
Åland Islands
Albania
Andorra

☐ Negate

Tick

endian

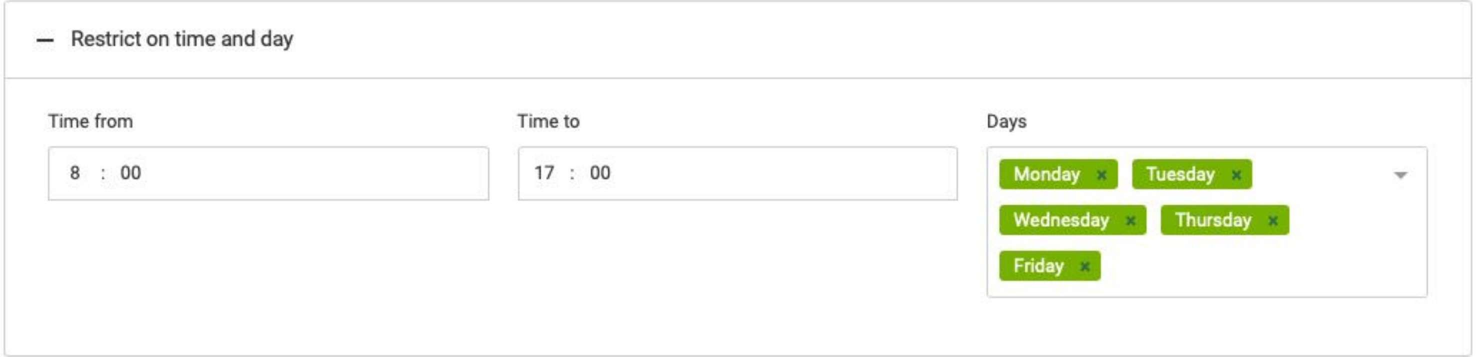
Secure everyThing

Module
Firewall

DNAT Tips & Tricks

NEW Time of Day / Day of Week Restrictions

You can create a DNAT rule that allows you to restrict rules based on a schedule using a combination of time of day and day of week. As an example, this can be useful for creating rulesets that apply different rules during business hours than non-business hours.



— Restrict on time and day

Time from: 8 : 00

Time to: 17 : 00

Days: Monday × Tuesday × Wednesday × Thursday × Friday ×

endian

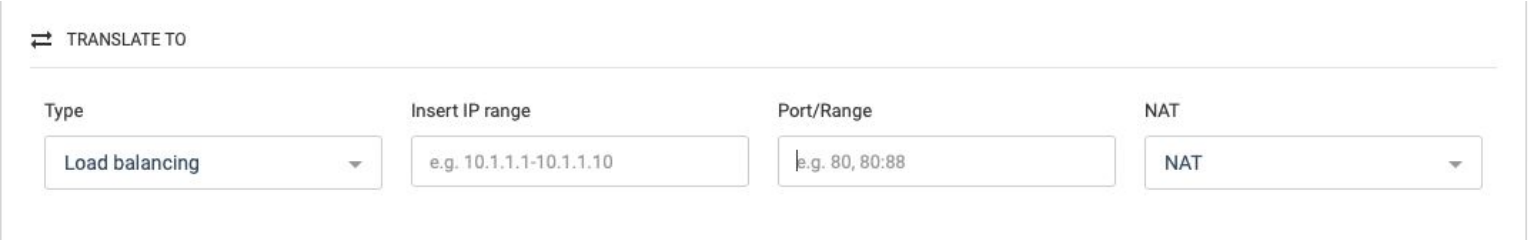
Secure everyThing

Module
Firewall

DNAT Tips & Tricks

Load Balancing

You can create a DNAT rule that allows you to send specific external traffic to a pool of internal resources utilizing a basic form of load balancing. Keep in mind that when using load balancing, the internal servers will be chosen randomly and there is no intelligence to know when a server becomes unavailable.



⇄ TRANSLATE TO

Type	Insert IP range	Port/Range	NAT
Load balancing	e.g. 10.1.1.1-10.1.1.10	e.g. 80, 80:88	NAT

endian

Secure everyThing

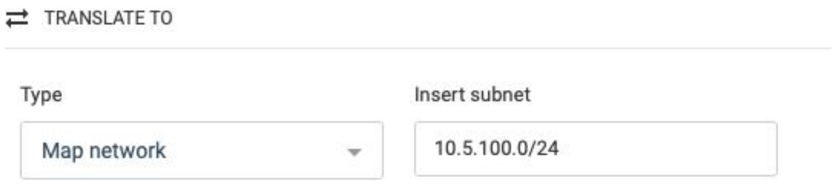
Module Firewall

DNAT Tips & Tricks

Map Networks

You can create a DNAT rule that allows you to perform a 1:1 map of an external subnet to an internal subnet. This can be very useful especially when you have to connect remote sites together via VPN that have overlapping (or duplicate) subnets.

Note: In order to map networks in both directions, you must also create a reverse SNAT rule that maps the internal network back to the external.



⇄ TRANSLATE TO

Type: Map network

Insert subnet: 10.5.100.0/24

endian

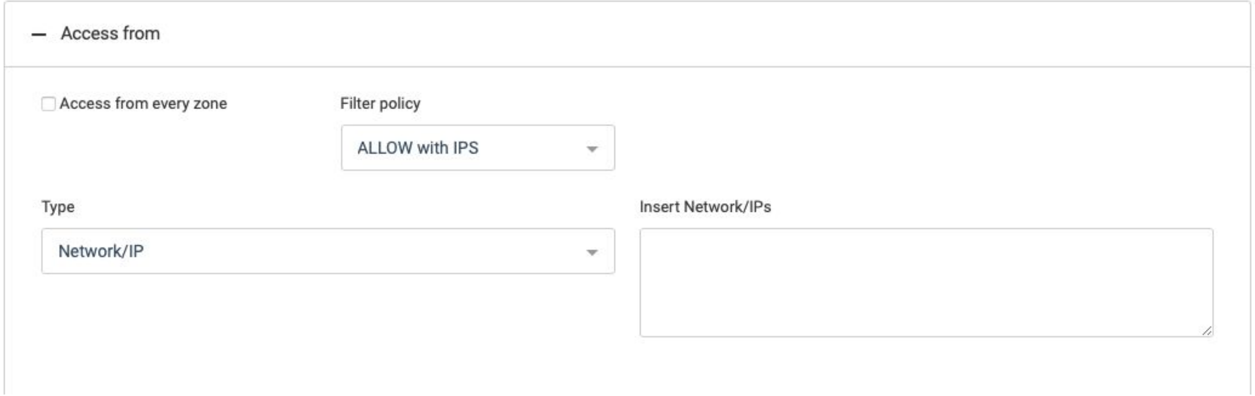
Secure everyThing

Module Firewall

DNAT Tips & Tricks

Restricted Access

When you create a DNAT rule, by default the Endian allows access to that rule from any outside IP. In some instances, you may wish to restrict which outside networks / IP addresses can access a certain DNAT rule to provide enhanced security.



— Access from

☐ Access from every zone

Filter policy: ALLOW with IPS

Type: Network/IP

Insert Network/IPs

Source NAT (SNAT)

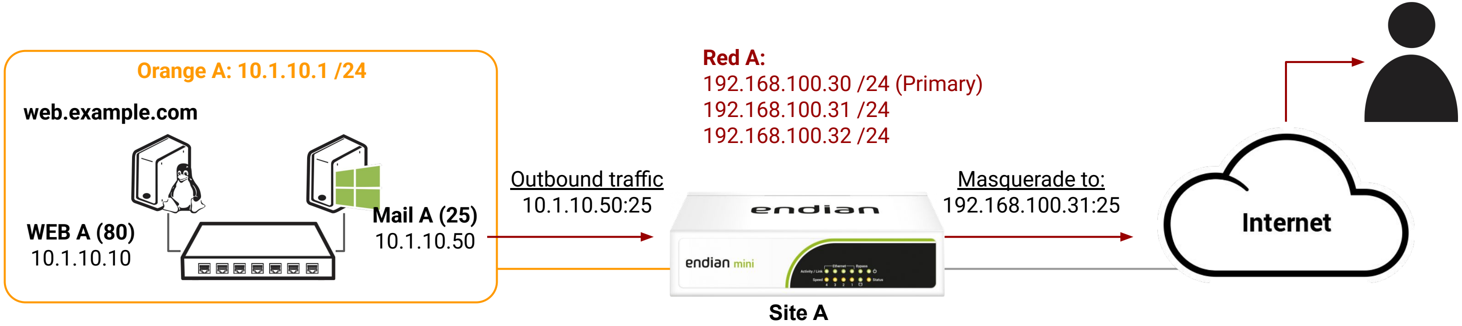
The Source NAT (SNAT) provides the ability to rewrite the source IP and/or port of outbound traffic to external networks. This can be useful when one has multiple external IP addresses and needs to manipulate certain internal traffic to appear to come from specific external IP addresses. An example where this is useful is when administering outbound traffic for mail servers that must pass a reverse DNS query for an IP address other than the default Red IP (see below).

Note: By default all outbound Internet traffic will automatically Source NAT to the Primary IP on the Red (main uplink) interface. This is a default masquerading rule created in order to hide the internal, private IP addresses.

endian
Secure everyThing

Module
Firewall

Source NAT (SNAT)

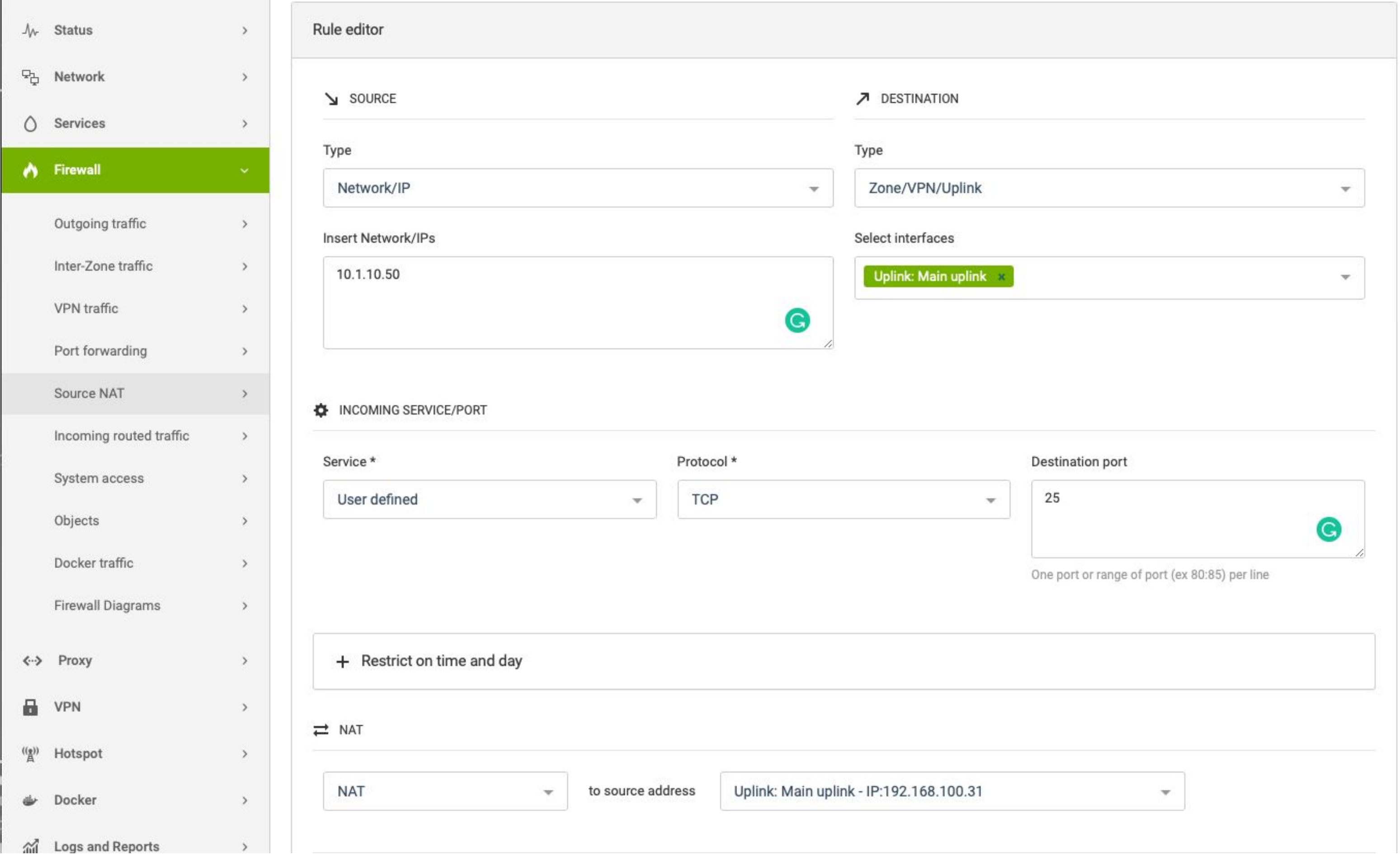


Example: Let’s use a sample network and add a SNAT rule that maps SMTP (TCP/25) traffic from an internal mail server (10.1.10.50) to an existing external IP address (192.168.100.31).

endian

Secure everyThing

Module Firewall



Rule editor

SOURCE

Type: Network/IP

Insert Network/IPs: 10.1.10.50

DESTINATION

Type: Zone/VPN/Uplink

Select interfaces: Uplink: Main uplink ×

INCOMING SERVICE/PORT

Service *: User defined

Protocol *: TCP

Destination port: 25

One port or range of port (ex 80:85) per line

+ Restrict on time and day

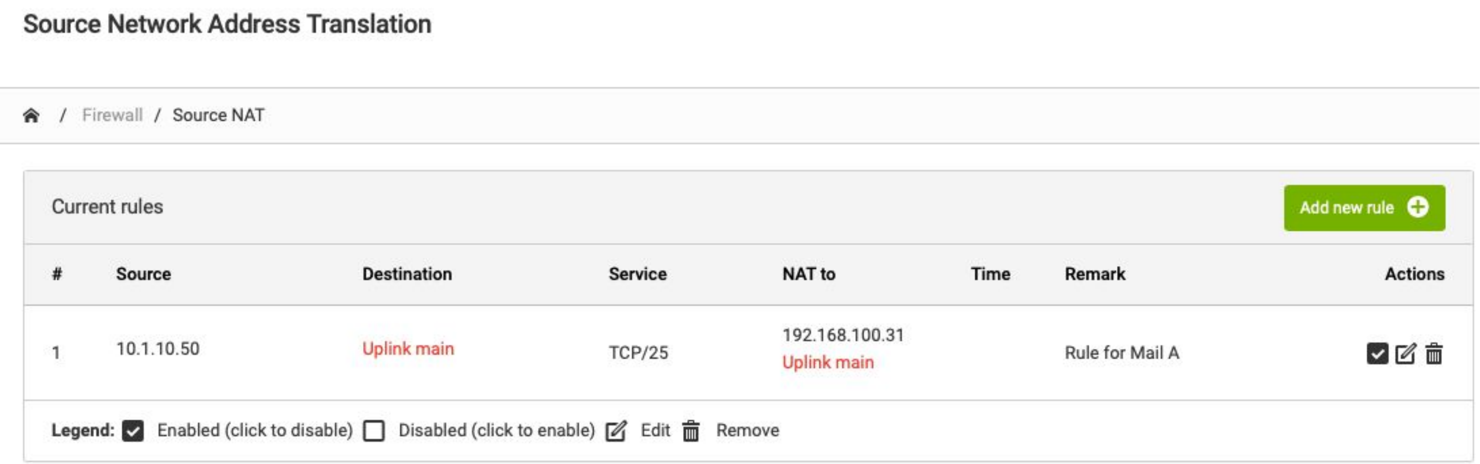
NAT

NAT to source address Uplink: Main uplink - IP:192.168.100.31

Source NAT - Example

endian
Secure everyThing

Module Firewall



Source Network Address Translation

🏠 / Firewall / Source NAT

Current rules

#	Source	Destination	Service	NAT to	Time	Remark	Actions
1	10.1.10.50	Uplink main	TCP/25	192.168.100.31 Uplink main		Rule for Mail A	☑ ✎ 🗑

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit 🗑 Remove

Source NAT - Example

Incoming Routed Firewall

The Incoming Routed firewall provides the ability to redirect incoming traffic destined for the Endian external interface to an internal network or zone. This can be used to route a public, external network through the Endian without having to NAT the traffic.

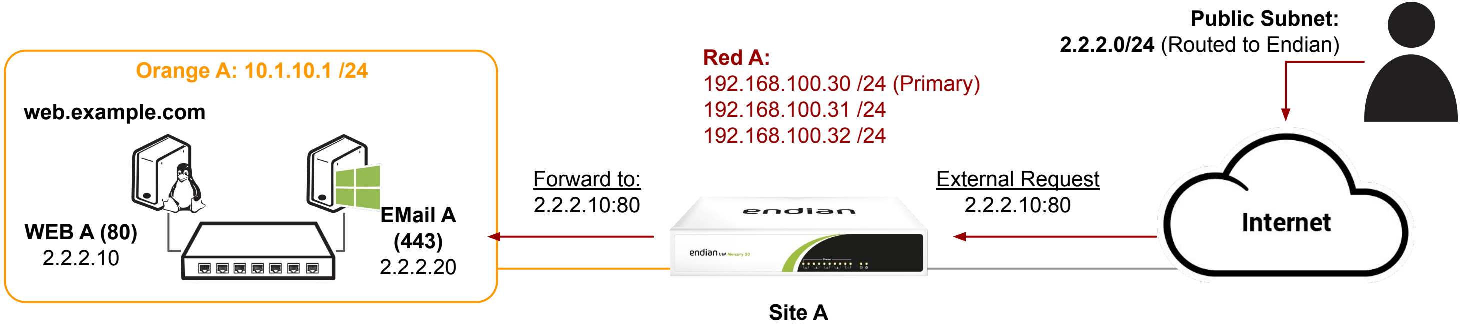
Since the Incoming Routed feature does not use NAT, your public (external) network will live on your hosted devices; thus every internal device will use a public network IP (and not a private IP).

Example: You wish to route the public network 2.2.2.0/24 to your Orange zone (interface). Every device inside the Orange zone will then directly be assigned an IP in the 2.2.2.0/24 network.

endian
Secure everyThing

Module Firewall

Incoming Routed Firewall

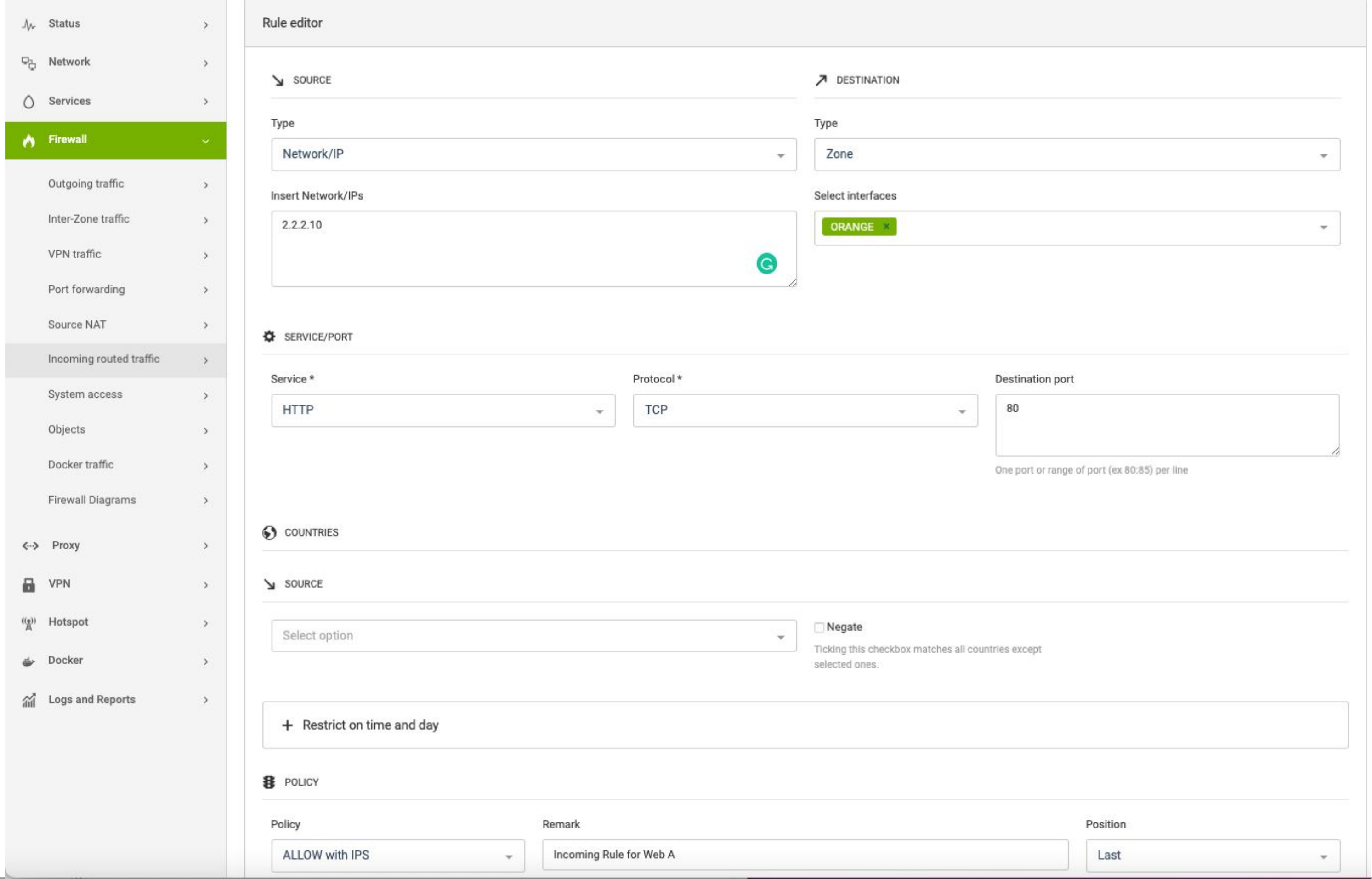


Example: Let’s use a sample network and add a Incoming rule that maps HTTP (TCP/80) traffic for a public IP (2.2.2.10) to a server in the Orange zone with that public IP assigned.

endian

Secure everyThing

Module
Firewall



Rule editor

SOURCE

Type: Network/IP

Insert Network/IPs: 2.2.2.10

DESTINATION

Type: Zone

Select interfaces: ORANGE ×

SERVICE/PORT

Service *: HTTP

Protocol *: TCP

Destination port: 80

One port or range of port (ex 80:85) per line

COUNTRIES

SOURCE

Select option

□ Negate

Ticking this checkbox matches all countries except selected ones.

+ Restrict on time and day

POLICY

Policy: ALLOW with IPS

Remark: Incoming Rule for Web A

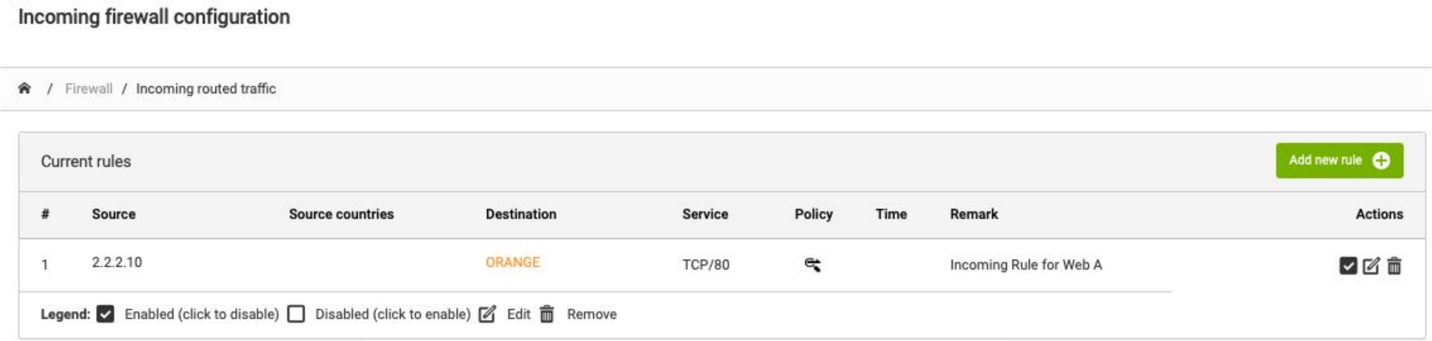
Position: Last

Incoming Routed - Example

endian

Secure everyThing

Module Firewall



Incoming firewall configuration

/ Firewall / Incoming routed traffic

Current rules

Add new rule ⊕

#	Source	Source countries	Destination	Service	Policy	Time	Remark	Actions
1	2.2.2.10		ORANGE	TCP/80			Incoming Rule for Web A	☑ ✎ 🗑

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit 🗑 Remove

Incoming Routed - Example

Outgoing Firewall

The Outgoing (or Egress) firewall provides the ability to filter outbound traffic originating from an internal, protected network. Using the outgoing firewall is highly recommended as it ensures that only traffic you explicitly approve is leaving your internal networks. By default, the outgoing firewall is enabled with a limited, common set of applications approved to leave specific network zones.

Warning: Always keep in mind that any traffic not explicitly allowed will be denied!! You can also choose to disable the outgoing firewall to ensure all outbound traffic passes through the Endian.

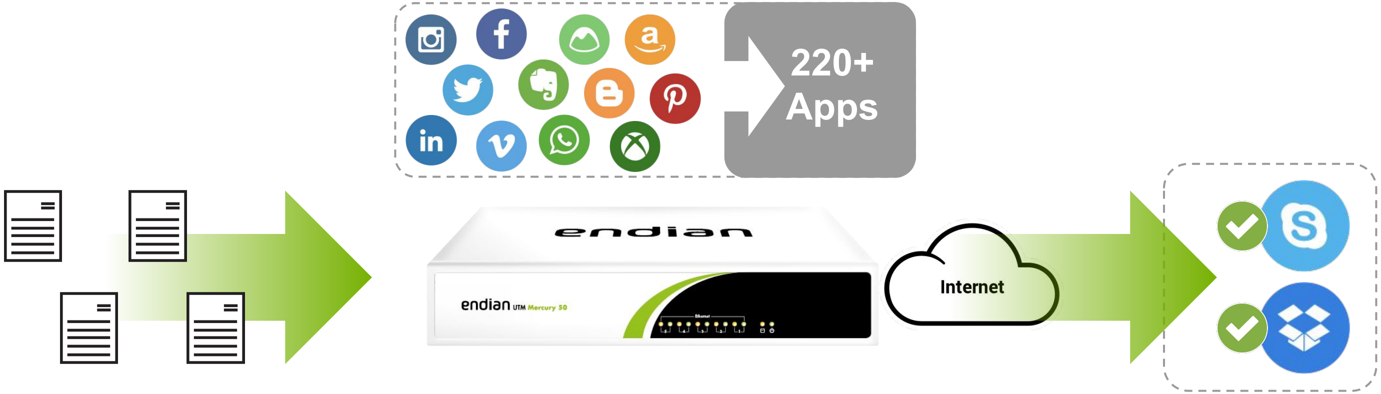
endian
Secure everyThing

Module
Firewall

Outgoing Firewall

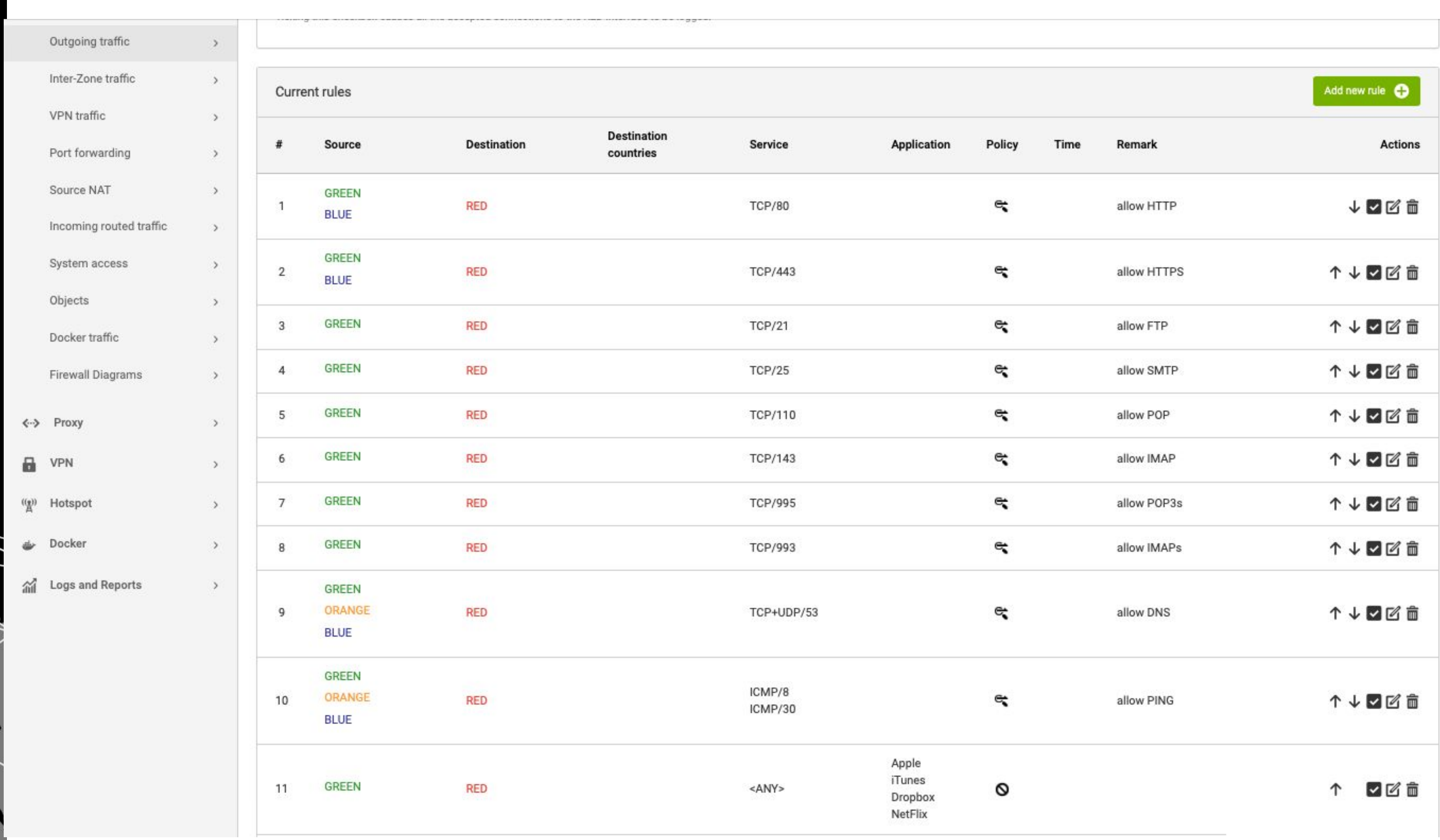
Application Control

Endian has added the ability to control outbound traffic by application. It does this using deep-packet inspection technology called nDPI (powered by NTOP) that can recognize 220+ applications regardless of port used by an application.



endian
Secure everyThing

Module Firewall



Current rules

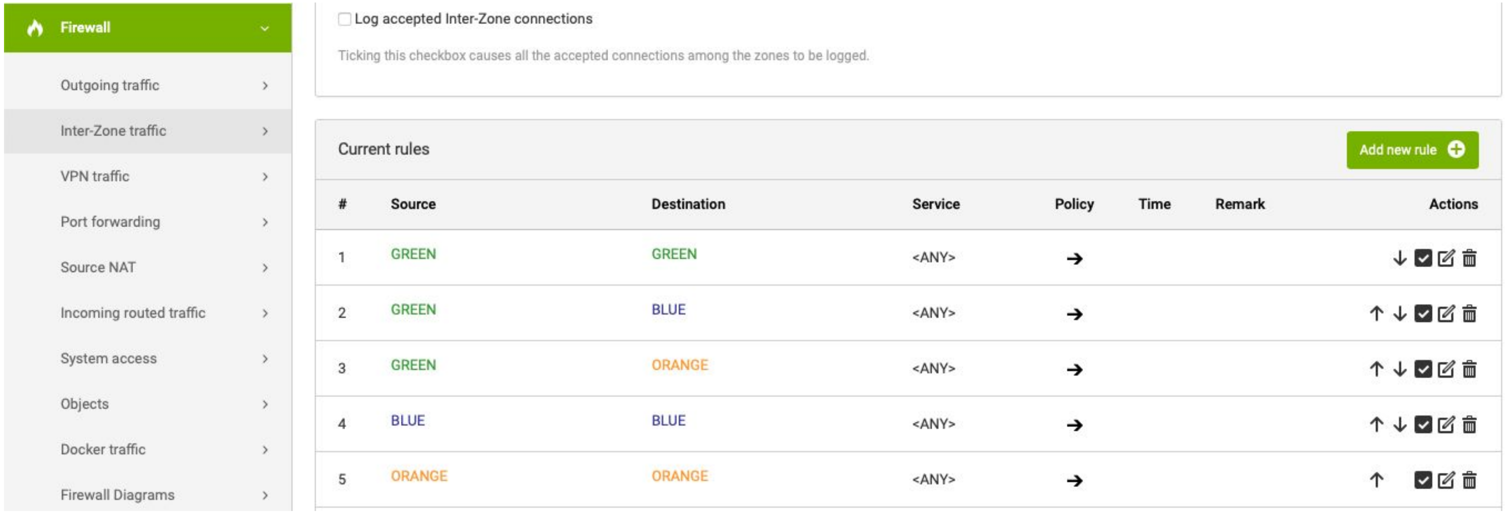
#	Source	Destination	Destination countries	Service	Application	Policy	Time	Remark	Actions
1	GREEN BLUE	RED		TCP/80		⇄		allow HTTP	↓ ☑ ✎ 🗑
2	GREEN BLUE	RED		TCP/443		⇄		allow HTTPS	↑ ↓ ☑ ✎ 🗑
3	GREEN	RED		TCP/21		⇄		allow FTP	↑ ↓ ☑ ✎ 🗑
4	GREEN	RED		TCP/25		⇄		allow SMTP	↑ ↓ ☑ ✎ 🗑
5	GREEN	RED		TCP/110		⇄		allow POP	↑ ↓ ☑ ✎ 🗑
6	GREEN	RED		TCP/143		⇄		allow IMAP	↑ ↓ ☑ ✎ 🗑
7	GREEN	RED		TCP/995		⇄		allow POP3s	↑ ↓ ☑ ✎ 🗑
8	GREEN	RED		TCP/993		⇄		allow IMAPs	↑ ↓ ☑ ✎ 🗑
9	GREEN ORANGE BLUE	RED		TCP+UDP/53		⇄		allow DNS	↑ ↓ ☑ ✎ 🗑
10	GREEN ORANGE BLUE	RED		ICMP/8 ICMP/30		⇄		allow PING	↑ ↓ ☑ ✎ 🗑
11	GREEN	RED		<ANY>	Apple iTunes Dropbox NetFlix	⊘			↑ ☑ ✎ 🗑

Outgoing Firewall

endian

Secure everyThing

Module Firewall



□ Log accepted Inter-Zone connections

Ticking this checkbox causes all the accepted connections among the zones to be logged.

Current rules

#	Source	Destination	Service	Policy	Time	Remark	Actions
1	GREEN	GREEN	<ANY>	→			↓ ☑ ✎ 🗑
2	GREEN	BLUE	<ANY>	→			↑ ↓ ☑ ✎ 🗑
3	GREEN	ORANGE	<ANY>	→			↑ ↓ ☑ ✎ 🗑
4	BLUE	BLUE	<ANY>	→			↑ ↓ ☑ ✎ 🗑
5	ORANGE	ORANGE	<ANY>	→			↑ ☑ ✎ 🗑

The Inter-Zone firewall provides for filtering capability between the internal network zones of Endian. For the 3 Endian legacy network zones, these are configured based on the predefined security levels of each network zone (i.e. Green = most protected and Orange/Blue = less protected).

Inter-Zone Firewall

VPN Firewall

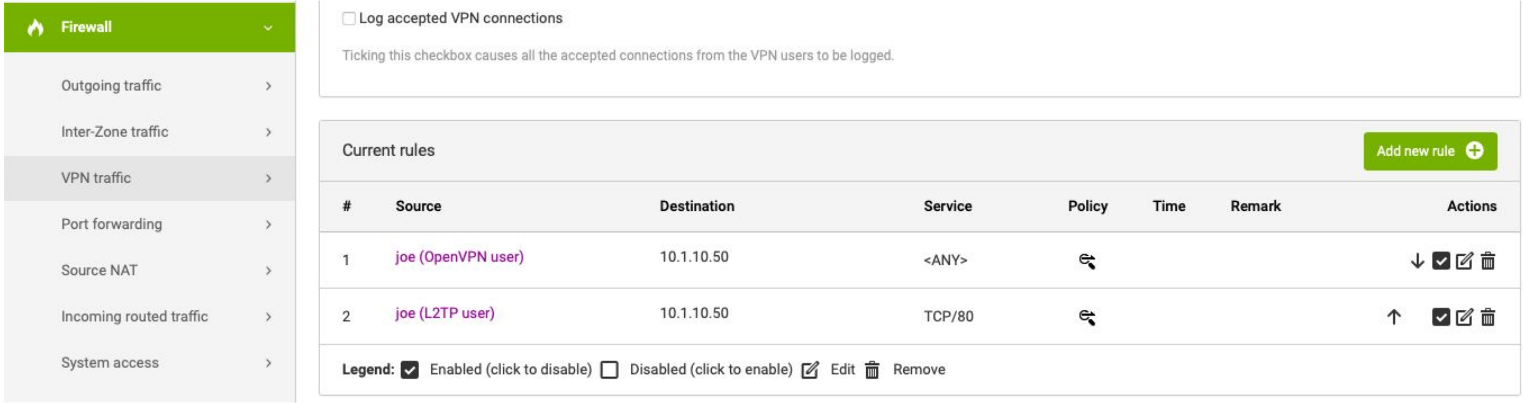
The VPN firewall provides the capability to explicitly filter VPN users access to internal resources. By default, the VPN firewall is disabled and all VPN users are automatically allowed access to any internal resources as if they were directly connected to the Green network. The rules themselves are relatively straightforward to build and have the same format as any other firewall rule.

Warning: When the VPN firewall is **enabled**, all VPN traffic not explicitly defined is blocked which means you must create rules for ALL traffic you wish to allow.

Warning: The VPN firewall only applies to users connected through VPN. The Outgoing and Inter-zone firewall do not apply to VPN users so the only place to filter VPN users is within the VPN firewall

endian
Secure everyThing

Module Firewall



□ Log accepted VPN connections

Ticking this checkbox causes all the accepted connections from the VPN users to be logged.

Current rules

#	Source	Destination	Service	Policy	Time	Remark	Actions
1	joe (OpenVPN user)	10.1.10.50	<ANY>				↓ ☑ ✎ 🗑
2	joe (L2TP user)	10.1.10.50	TCP/80				↑ ☑ ✎ 🗑

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit 🗑 Remove

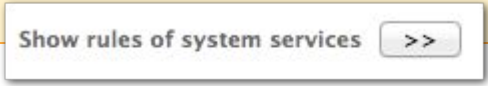
Note: You must create separate rules for SSL (OpenVPN) users and L2TP users. This also means you can provide different rulesets depending on which VPN application the client is using.

VPN Firewall

System Access Firewall

The System firewall provides granular filtering capability over access to services running on the Endian device directly (e.g. HTTPS, SSH, DNS, etc). By default, no services are made available externally including all management services (Web & SSH) to eliminate direct outside access to the device.

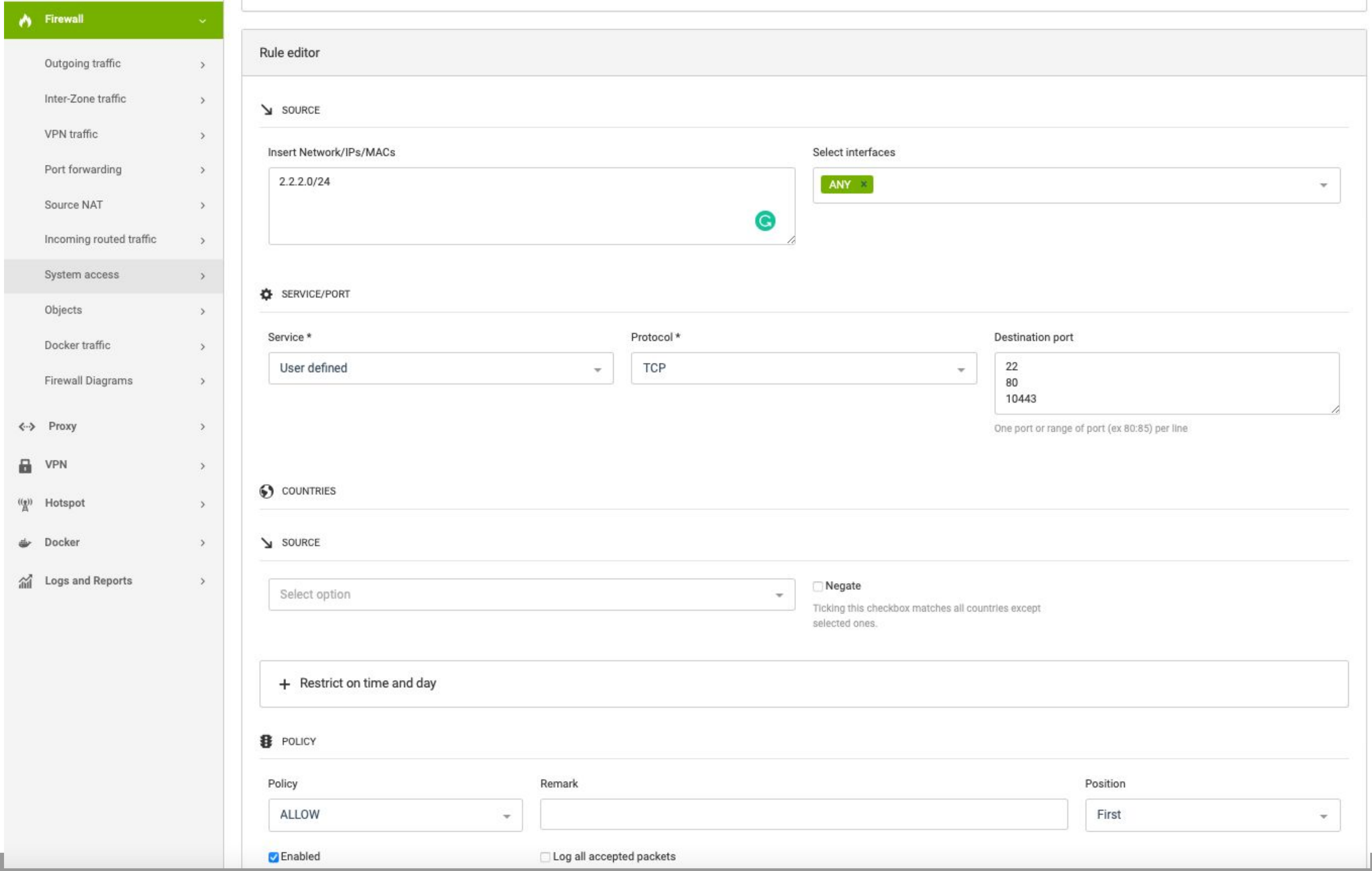
Warning: All relevant System Access rules needed by the Endian UTM to provide any user-enabled functionality will automatically be added to the System firewall. You can view these at any time by selecting the ‘Show rules of system services’ button.



endian

Secure everyThing

Module Firewall



Rule editor

SOURCE

Insert Network/IPs/MACs: 2.2.2.0/24

Select interfaces: ANY

SERVICE/PORT

Service *: User defined

Protocol *: TCP

Destination port:

```
22
80
10443
```

One port or range of port (ex 80:85) per line

COUNTRIES

SOURCE

Select option

□ Negate

Ticking this checkbox matches all countries except selected ones.

+ Restrict on time and day

POLICY

Policy: ALLOW

Remark:

Position: First

☑ Enabled

□ Log all accepted packets

VPN Firewall

endian

Secure everyThing

Module
Firewall

NEW Docker Firewall

The new Docker system allows administrators to run microservices / applications in containers which run on the Endian appliance itself. You can thus control access to both incoming and outgoing traffic to any of the Docker containers.

Note: The Docker system and its architecture are beyond the scope of this course and thus we won’t go into detail on this firewall component.

Thanks

End :: Module Firewall