

### Rule 1 :

Cette règle est conçue pour autoriser le trafic TCP/UDP depuis les sous-réseaux LAN vers n'importe quelle destination sur les ports HTTP (80) et HTTPS (443), facilitant ainsi l'accès à Internet pour les employés. La journalisation est facultative, et la règle est spécifique à IPv4. L'interface ressemble à celle des systèmes de gestion de pare-feu comme pfSense ou OPNsense.

Firewall / Rules / Edit

Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP/UDP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

LAN subnets

Source Address

/

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination

☐ Invert match

Any

Destination Address

/

Destination Port Range

From

HTTP (80)

Custom

To

HTTPS (443)

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

Autoriser navigation web pour employés

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Activate Windows

Go to Settings to activate Windows.

Rule 2 :

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

WAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Any

Source Address

Activate Windows

Go to Settings to activate Windows.

## Source

Source

☐ Invert match

Any

Source Address

/

▼

 Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

## Destination

Destination

☐ Invert match

WAN address

Destination Address

/

▼

**Destination Port Range**

From HTTP (80 ▼)

Custom

To HTTPS (4 ▼)

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

## Extra Options

**Log** ☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description**

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Activate Windows

Go to Settings to activate Windows.

**Advanced Options**

 Display Advanced

Rule 3 :

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

WAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

UDP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Any

Source Address /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination

☐ Invert match

WAN address

Destination Address /

Destination Port Range

OpenVPN

From

Custom

OpenVPN

To

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

Allow VPN for remote work

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Rule 4 :

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

LAN address

Source Address

/

Display Advanced

Activate Windows

Go to Settings to activate Windows.

Source

Source

☐ Invert match

LAN address

Source Address

/

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination

☐ Invert match

OPT1 subnets

Destination Address

/

Destination Port Range

SSH (22)

From

Custom

To

SSH (22)

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description

Accès SSH admin vers DMZ

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Save

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\islem> ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (C:\Users\islem/.ssh/id_ed25519):
Created directory 'C:\Users\islem/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\islem/.ssh/id_ed25519
Your public key has been saved in C:\Users\islem/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:cXTUG7LW2okpm0cbI80MQR7yHmWAN75PMupIf7pgG1A islem@DESKTOP-S7C4FKE
The key's randomart image is:
+--[ED25519 256]--+
|      .o=o=.      |
|      .+=. o      |
|    E   .o=o + o   |
|      .  +o.o o    |
|      S .B = .    |
|      * % o       |
|    . + . @ +     |
|      = +. + +     |
|    . ..=+ .      |
+-----[SHA256]-----+
PS C:\Users\islem>
```

Rule 6 :




IP

Ports

URLs

All

Firewall Aliases IP


Name	Type	Values	Description	Actions
Blocked_Social_Media	Host(s)	facebook.com, instagram.com		  

+

 Add 

↑

 Import





WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Aliases / Edit

?

Properties

Name

Blocked\_Social\_Media

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and \_".

Description

A description may be entered here for administrative reference (not parsed).

Type

Host(s)

Host(s)

Hint

Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN

facebook.com

Entry added Fri, 09 May 2025 15:58:21 +0000

Delete

IP or FQDN

instagram.com

Entry added Fri, 09 May 2025 15:58:21 +0000

Delete

Save

Export to file

Add Host

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

LAN subnets

Source Address

/

Destination

Destination

☐ Invert match

Address or Alias

TeamsAlias

/

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

Allow Microsoft Teams

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall

Activate Windows

Go to Settings to activate Windows.

Rule 8 :



Edit Firewall Rule

Action

Block

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

LAN subnets

Source Address

/

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination

☐ Invert match

Any

Destination Address

/

Destination Port Range

Telnet (23)

From

Custom

Telnet (23)

To

Custom

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination

☐ Invert match

Any

Destination Address

/

Destination Port Range

Telnet (23)

From

Custom

Telnet (23)

To

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

Block Telnet

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Save

## Edit Firewall Rule

**Action**

Block

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled**☐ Disable this rule

Set this option to disable this rule without removing it from the list.

**Interface**

LAN

Choose the interface from which packets must come to match this rule.

**Address Family**

IPv4

Select the Internet Protocol version this rule applies to.

**Protocol**

TCP

Choose which IP protocol this rule should match.

## Source

**Source**☐ Invert match

LAN subnets

Source Address

/

▼

 Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Activate Windows

Go to Settings to activate Windows.

## Source

**Source**☐ Invert match

LAN subnets

Source Address

/

▼

 Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

## Destination

**Destination**☐ Invert match

Any

Destination Address

/

▼

**Destination Port Range**

FTP (21)

From

Custom

FTP (21)

To

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

## Extra Options

**Log**☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description**

Block FTP

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options** Display Advanced Save



Properties

Name

EntertainmentSites

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and \_".

Description

A description may be entered here for administrative reference (not parsed).

Type

Host(s)

Host(s)

Hint

Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN	youtube.com	Description	Delete
	netflix.com	Description	Delete
	primevideo.com	Description	Delete
	hulu.com	Description	Delete
	twitch.tv	Description	Delete
	tiktok.com	Description	Delete

Save

+ Add Host

Activate Windows  
Go to Settings to activate Windows.

Time

0

00

23

59

Start HrsStart MinsStop HrsStop Mins

Select the time range for the day(s) selected on the Month(s) above. A full day is 0:00-23:59.

Time range description

A description may be entered here for administrative reference (not parsed).

+ Add Time

Clear selection

Configured Ranges

Mon	14:30	18:00		Delete
Day(s)	Start time	Stop time	Description	
Mon	8:00	12:00		Delete
Day(s)	Start time	Stop time	Description	
Tues	8:00	12:00		Delete
Day(s)	Start time	Stop time	Description	
Tues	14:30	18:00		Delete
Day(s)	Start time	Stop time	Description	
Wed - Fri	8:00	12:00		Delete
Day(s)	Start time	Stop time	Description	
Wed - Fri	14:30	18:00		Delete
Day(s)	Start time	Stop time	Description	

Save

Activate Windows  
Go to Settings to activate Windows.

Edit Firewall Rule

Action

Block

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

LAN subnets

Source Address

/

Destination

Destination

☐ Invert match

Address or Alias

EntertainmentSites

/

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description

Block entertainment sites during working hours

Extra Options

Log

☐ Log packets that are handled by this rule


Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description

Block entertainment sites during working hours

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options



Advanced Options

Source OS

Any

Note: this only works for TCP rules. General OS choice matches all subtypes.

Diffserv Code Point

Allow IP options

☐ Allow packets with IP options to pass. Otherwise they are blocked by default. This is usually only seen with multicast traffic.

Disable reply-to

☐ Disable auto generated reply-to for this rule.

Tag

A packet matching this rule can be marked and this mark used to match on other NAT/filter rules. It is called **Policy filtering**.

Tagged

☐ Invert

Tagged

Match a mark placed on a packet by a different rule with the Tag option. Check Invert to match packets which do not contain this tag.

Max. states

Maximum state entries this rule can create.

Max. src nodes

Maximum number of unique source hosts.

Choose 802.1p priority to apply.

Schedule

WorkHours

Leave as 'none' to leave the rule enabled all the time.

Gateway

Default

Rule 10 :

Edit Firewall Rule

Action

Block

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

OPT1

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

OPT1 subnets

Source Address

/

Destination

Destination

☐ Invert match

LAN subnets

Destination Address

/

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see

Source

Source

☐ Invert match

OPT1 subnets

Source Address

/

Destination

Destination

☐ Invert match

LAN subnets

Destination Address

/

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description

Block traffic from DMZ to LAN

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Save

Activate Windows  
Go to Settings to activate Windows

Activate Windows