- [Instructeur] Bonjour
tout le monde, nous allons
examiner la partie pare-feu
de notre pare-feu et routeur sans fil CISCO.
Votre routeur doit également avoir des fonctionnalités similaires
à celles que nous allons présenter aujourd'hui.
Ce routeur/pare-feu est connecté au web
via le port Internet. Pour en savoir plus,
je clique sur Status et
j'accède à ce tableau de bord
dans lequel nous pouvons voir que le port WAN est connecté.
Il est allumé et vert. Ce tableau de bord donne de nombreuses informations.
Par exemple, il indique qu'un ordinateur est connecté
au port 1 du port LAN.
Mon ordinateur se trouve derrière ce pare-feu de routeur
sur le réseau local. Il s'agit du réseau interne.
Nous allons pouvoir configurer
ce réseau interne et ce pare-feu avec des règles.
Ce pare-feu prend en charge une zone démilitarisée ou DMZ.
Il s'agit d'un sous-réseau qui va être ouvert au public,
mais qui est localisé derrière le pare-feu.
Une DMZ nous permet de rediriger les paquets
vers l'adresse IP de mon port WAN au port LAN d'un périphérique spécifique.
C'est ce que nous allons faire aujourd'hui.
Nous pouvons également configurer des règles de pare-feu
pour définir le type de trafic qui peut atteindre la zone DMZ.
La DMZ n'est donc pas une porte ouverte pour toutes les connexions réseau.
C'est parti.
Nous allons tout d'abord
accéder à Networking,
puis à LAN. Même si nous configurons un pare-feu,
les paramètres de configuration DMZ
se trouvent sous LAN.
Je clique sur DMZ Host.
Il y a très peu d'options.
Tout d'abord nous allons activer la DMZ.
Je clique donc sur Enable pour la zone DMZ.
Ensuite, nous devons définir
l'adresse IP de l'hôte qui va être une adresse IP statique fixe
pour le périphérique final qui va fonctionner dans la DMZ.
Je vais donc indiquer 192.168.1.200,
qui sera l'adresse IP du périphérique final qui devra être accessible depuis l'extérieur.
Je clique ensuite sur Save
pour enregistrer les paramètres.

Ensuite, il peut être utile d'examiner
les paramètres de transfert de port, qui se trouvent dans la section pare-feu.
Je clique sur Firewall et
nous accédons directement au transfert de port unique.
Le transfert de port nous permet de rediriger le trafic provenant d'Internet.
Nous recherchons alors un trafic spécifique
arrivant sur le port WAN
et nous le transférons vers un périphérique interne sur l'un des ports LAN.
Par défaut,
des éléments sont déjà créés, mais ils ne sont pas activés,
car l'option Enable n'est pas cochée et il n'y a pas d'adresse IP interne
vers laquelle transférer le trafic.
Il s'agit d'une fonctionnalité très pratique pour les services d'hébergement
et les terminaux qui doivent être accessibles depuis l'extérieur,
par exemple pour accéder
à des périphériques internes tels que des caméras IP,
des serveurs de jeu et tout autre périphérique
sur votre réseau interne.
Maintenant nous allons créer
notre règle de transfert de port.
Je vais nommer la mienne, IPcam1,
puis je choisis
le port externe auquel les internautes vont accéder
sur le port WAN de mon routeur.
Par exemple, imaginons que
des personnes ciblent mon adresse IP WAN avec le numéro de port 8090.
Lorsque le trafic accède au port WAN sur le port 8090,
nous allons faire en sorte qu'il cible un port interne en cours d'exécution
sur notre caméra IP.
Il peut s'agir par exemple du port 1044.
Je choisis ensuite le protocole utilisé par ma caméra IP,
probablement UDP.
Pour l'interface WAN, je vais choisir Ethernet.
3G est possible, car le pare-feu/routeur VPN sans fil
prend en charge une connexion de données cellulaires 3G pour le WAN.
Comme nous n'en avons pas besoin, nous allons choisir Ethernet, qui est le port WAN
auquel nous sommes connectés.
Pour finir, je dois saisir l'adresse IP privée de la caméra IP.
Il s'agit de 192.168.1.150.
Je vais maintenant activer cette règle
en cochant la case Enable.
Puis, je vais tout en bas de l'écran
et je clique sur Save.
Poursuivons

en examinant quelques-uns des paramètres de base
de notre pare-feu.
Pour ce faire, je clique sur Basic Settings.
Lorsque l'écran se charge,
nous allons examiner certains paramètres de sécurité par défaut
qui ont été définis.
En haut se trouvent des paramètres de protection contre l'usurpation d'identité
afin de contrer des utilisateurs internes
qui essaient de se faire passer pour un périphérique réseau.
Ce paramètre est activé par défaut.
Nous disposons également d'une protection contre les dénis de service,
qui empêche notre pare-feu d'être submergé
par du trafic malveillant.
Nous bloquons même les requêtes ping,
car nous n'allons pas répondre aux personnes
qui essaient d'envoyer une requête ping à notre adresse Internet sur le port WAN de notre routeur.
Un peu plus bas, nous pouvons voir que
seul un administrateur est autorisé à configurer notre pare-feu
via une session HTTPS chiffrée.
Il s'agit de cette option Remote Access.
Si nous activons ces paramètres distants,
un administrateur externe sur Internet
pourrait accéder à distance
à notre routeur
et modifier sa configuration.
Il y a ici plusieurs paramètres de sécurité
permettant d'autoriser l'accès à distance à des adresses IP spécifiques publiques,
ainsi que de sélectionner un port d'écoute
pour le port WAN.
Toutefois, cela peut s'avérer risqué.
Si vous choisissez cette option,
veillez à ce que votre mot de passe ou phrase secrète soit très complexe.
En bas de l'écran, nous allons maintenant
nous intéresser à UPnP, qui signifie Universal Plug and Play.
Ce protocole permet la détection automatique des périphériques
qui peuvent communiquer avec le pare-feu
et même modifier sa configuration
pour autoriser l'accès des équipements
à l'extérieur du WAN,
en utilisant pour cela des fonctionnalités telles que le transfert de port.
Bien que les paramètres UPnP peuvent être pratiques,
il est préférable que
vous configuriez vos règles de pare-feu et le transfert de port vous-même.

De plus, si nous voulons contrôler plus précisément le trafic interne,
en particulier le trafic voulant accéder au web,
c'est possible.
J'accède à la section des règles d'accès
où se trouve cette zone spéciale me permettant d'ajouter des lignes de règles.
Par exemple, en cliquant sur Add Row,
je peux choisir le type de connexion,
entrante ou sortante.
Par exemple, connexion WAN entrante vers le LAN.
Je peux définir une action à appliquer
concernant ce trafic.
Nous pouvons également programmer
quand cette action doit avoir lieu.
Concernant les services, nous pouvons choisir le type de trafic.
Nous pouvons même le définir plus précisément
à l'aide de la section de configuration des services.
Nous pouvons définir la source, c'est-à-dire l'emplacement sur Internet, par exemple « partout ».
Même chose pour la destination, à partir de quel emplacement dans mon réseau interne ?
Une seule adresse,
car il s'agit de trafic destiné à notre réseau local (LAN).
Ici nous indiquons les périphériques internes
qui ne doivent pas recevoir de trafic
d'un WAN public spécifique.
Nous pouvons activer cette règle à l'aide du bouton Enable,
et la consigner.
Ainsi, lorsque ce trafic se présente
et est abandonné, il est pris en compte
dans le pare-feu du routeur sans fil.
Nous allons maintenant nous intéresser au contenu
et au moyen d'empêcher les utilisateurs d'atteindre des sites web spécifiques.
Nous allons travailler de l'intérieur vers l'extérieur,
sur du contenu et non sur une adresse IP, contrairement à ce qui s'affiche ici.
Pour cela, nous accédons à Internet Access Policy.
Je clique.
Dans la fenêtre des politiques d'accès Internet, je peux créer plusieurs politiques
et les activer sur mon pare-feu.
Je peux approuver sur liste blanche
des éléments et en refuser d'autres sur liste noire. Voyons comment.
Je clique sur Add Row et je peux créer un nom de politique.
Appelons-la, par exemple, TEST.
Nous pouvons appliquer des actions
à cette politique TEST que nous sommes sur le point de créer :
bloquer selon un horaire, autoriser selon un horaire,

toujours bloquer ou toujours autoriser,
soit placer respectivement sur liste blanche ou sur liste noire.
Concernant l'option Apply Access Policy to the Following PCs ci-dessous,
vous pouvez choisir à qui cette politique s'applique.
Il peut s'agir d'une plage d'adresses,
d'une adresse IP spécifique ou même d'une adresse MAC de matériel.
Pour déterminer ce que nous voulons bloquer,
ci-dessous dans la zone relative au nom de domaine et mot-clé du site web,
nous cliquons sur Add Row
et nous pouvons bloquer un site à partir du nom de domaine
ou même d'un mot-clé.
Ainsi,
tous ces éléments
fonctionnent de concert pour identifier
les périphériques
et ce à quoi ils ont accès ou non.
Maintenant que nous avons examiné tous ces paramètres,
même si chaque pare-feu est un peu différent,
vous pouvez essayer
différentes configurations et vérifier les résultats
sur un PC interne de ce réseau.
Exercez-vous en dehors de vos horaires de travail
et vous deviendrez
un professionnel de l'informatique.