



Une formation
Alphorm.com

Formation Palo Alto *Firewall Troubleshooting*



Mohamed Anass EDDIK



Une formation
Alphorm.com

Cursus Palo Alto Networks





Une formation
Alphorm.com

Plan de la formation

Introduction

1. Connaître les outils ,ressources et CLI
2. Comprendre le comportement des flux
3. Définir la capture des paquets
4. Diagnostiquer les paquets
5. Gérer le trafic des hotes-entrants
6. Identifier le Transit Traffic
7. Diagnostiquer les services Systèmes
8. Gérer les certificats et le décryptage SSL
9. Diagnostiquer les User-ID
10. Diagnostiquer GlobalProtect

Conclusion



Une formation
Alphorm.com

Public concerné

Architectes de solution

Spécialistes du soutien

Administrateurs de pare-feu Palo Alto Networks



Connaissances requises

Routing, commutation, adressage IP et concepts de sécurité réseau

Configuration et administration du pare-feu Palo Alto Networks

6 mois d'expérience minimum avec les pare-feu Palo Alto Networks

Une formation
Alphorm.com



Formations pour les prérequis



Une formation
Alphorm.com



Présentation du Lab de travail



Mohamed Anass EDDIK



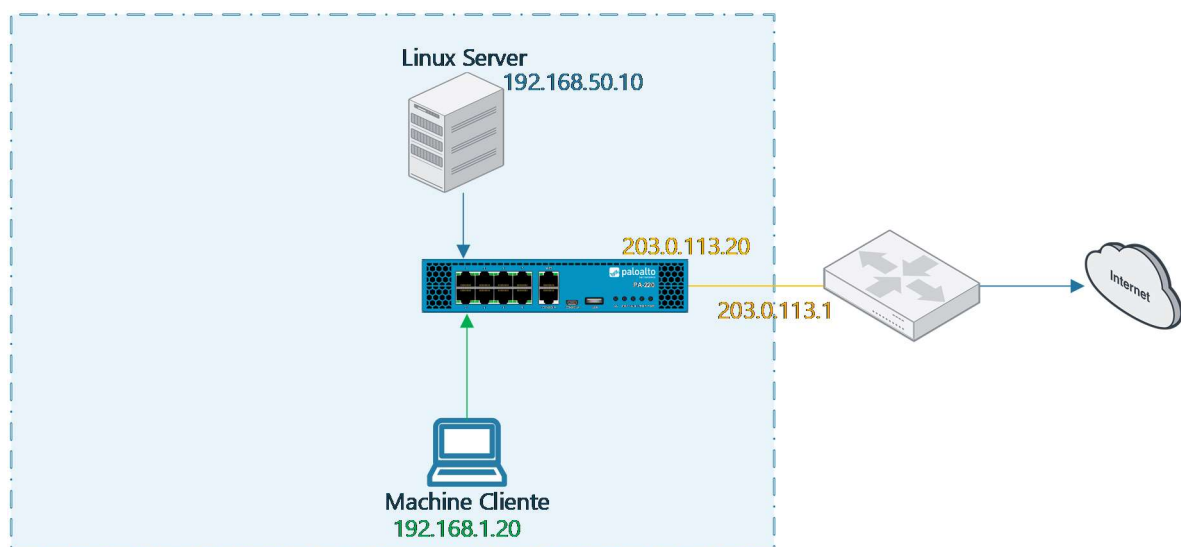
Firewall Troubleshooting

Plan

La topologie du LAB
Les prérequis du Lab
Les machines du LAB

Une formation
Alphorm.com

La topologie du LAB





Les prérequis du Lab

Une machine avec 16Go de RAM
VMware Workstation/Fusion (ou ESXi)
Une License Palo Alto Networks vm-50 ou vm-50 lite
Un serveur linux

Une formation
Alphorm.com



Les machines fournies

Une image d'un pare-feu Palo Alto
Un serveur Linux
Une machine client windows

Une formation
Alphorm.com



Découvrir les différents outils de diagnostic



Mohamed Anass EDDIK



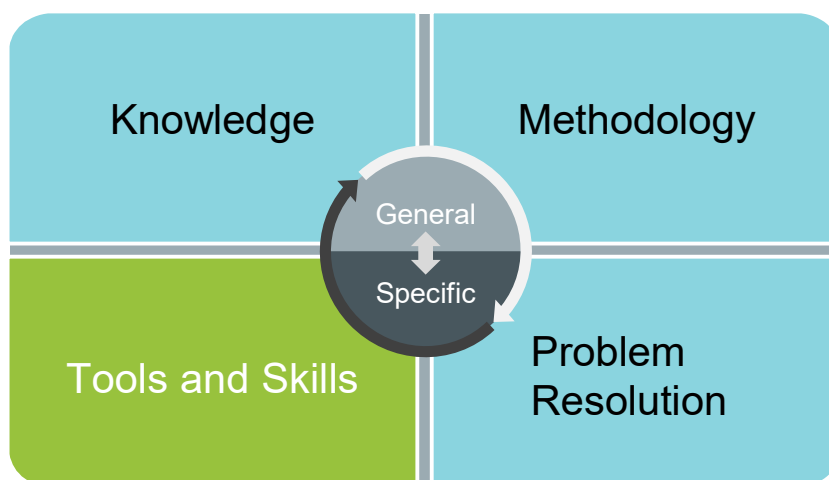
Plan

Activer le dépannage
Outils de diagnostique
Options d'information et de
support

Une formation
Alphorm.com



Activer le dépannage



Une formation
Alphorm.com



Outils de diagnostique

Au-niveau du PAN

Interface Web
CLI
Mode de maintenance

Outils externe

Informations de référence
Analyse et affichage des données
Connaissances et expérience individuelles
et la participation de la communauté

Compétences stratégiques

Reconnaissance des problèmes
Définition du problème
Sélection de solutions

Compétences tactiques

Methodology
Search and filtering
Log and pcap interpretation
CLI capability
Tool mastery

Une formation
Alphorm.com



Options d'information et de support

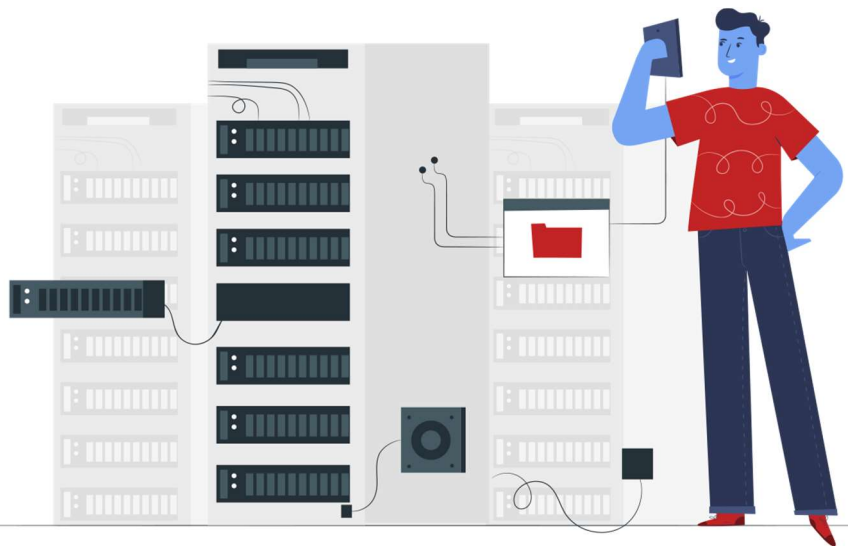
Fuel user Group
Live Community
Customer support Portal

Une formation
Alphorm.com



Firewall Troubleshooting

Démo



Une formation
Alphorm.com



Firewall Troubleshooting

Accéder au mode maintenance



Mohamed Anass EDDIK

Une formation
Alphorm.com



Une formation
Alphorm.com

Comprendre la structure des CLI



Mohamed Anass EDDIK



Une formation
Alphorm.com

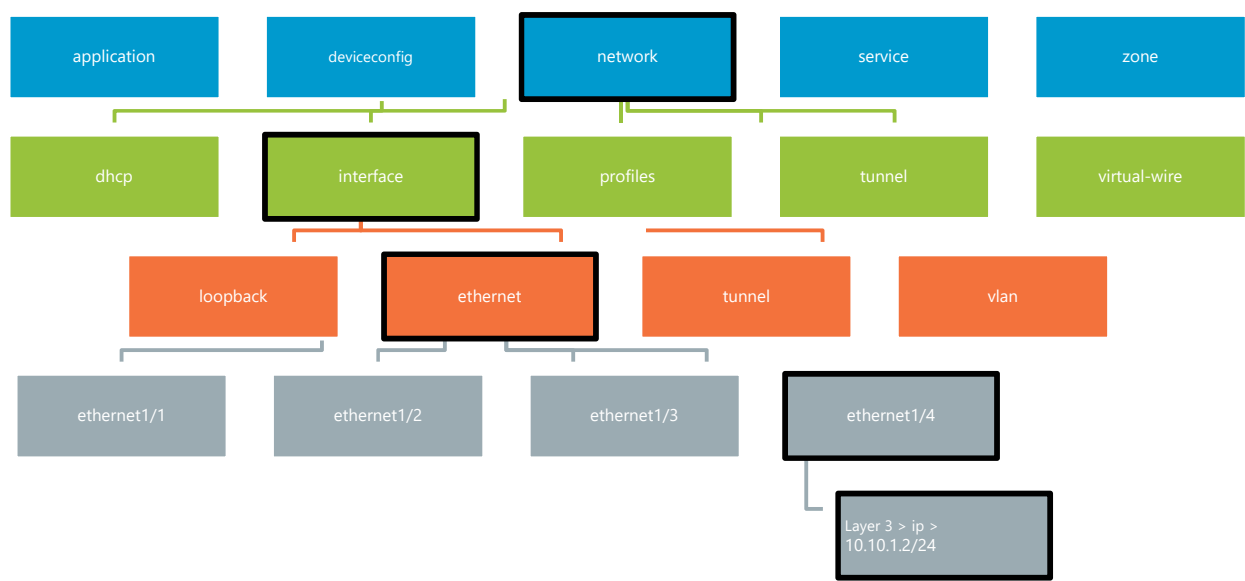
Plan

CLI Command Modes
Navigation de la hiérarchie
de Configuration

CLI Command Modes

	Operational Mode	Configuration Mode
Pour utiliser :	Default mode	configure command
Signe rapide :	>	#
Exemples de commandes :	show less test debug	show set or delete edit commit
Context de travail variable :	No	Yes, via edit command
Effet opérationnel :	Immediate	After commit
Caractéristiques partagées :	Role-based access control	
	Autocomplete	
	Suggestions	
	Short explanations for options	

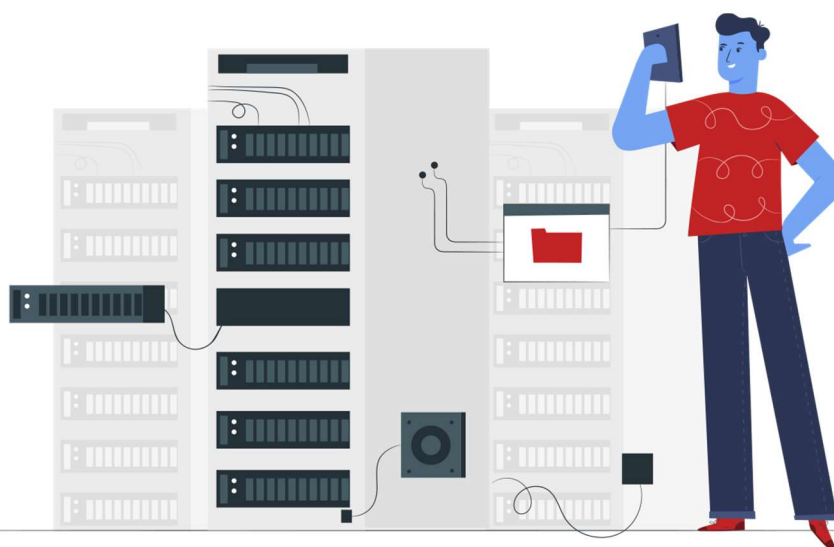
Navigation de la Hiérarchie de Configuration





Firewall Troubleshooting

Démo



Une formation
Alphorm.com



Firewall Troubleshooting

Afficher et naviguer au niveau des données



Mohamed Anass EDDIK

Une formation
Alphorm.com

CLI Configuration Display Formats

Default (Hjson)	XML	Set Commands
<pre>dns-proxy { proxy-xsn-internal-dns { cache { max-ttl { enabled yes; time-to-live 21600; } enabled yes; cache-edns no; } default { primary 8.8.8.8; secondary 4.2.2.2; } tcp-queries { enabled no; } interface ethernet1/2; enabled yes; } }</pre>	<pre><response status="success" code="19"> <result total-count="1" count="1"> <dns-proxy> <entry name="proxy-xsn-internal-dns"> <cache> <max-ttl> <enabled>yes</enabled> <time-to-live>21600</time-to-live> </max-ttl> <enabled>yes</enabled> <cache-edns>no</cache-edns> </cache> <default> <primary>8.8.8.8</primary> <secondary>4.2.2.2</secondary> </default> <tcp-queries> <enabled>no</enabled> </tcp-queries> </entry> </dns-proxy> </result> </response></pre>	<pre>set network dns-proxy proxy-xsn-internal-dns cache max-ttl enabled yes set network dns-proxy proxy-xsn-internal-dns cache max-ttl time-to-live 21600 set network dns-proxy proxy-xsn-internal-dns cache enabled yes set network dns-proxy proxy-xsn-internal-dns cache cache-edns no set network dns-proxy proxy-xsn-internal-dns default primary 8.8.8.8 set network dns-proxy proxy-xsn-internal-dns default secondary 4.2.2.2 set network dns-proxy proxy-xsn-internal-dns tcp-queries enabled no set network dns-proxy proxy-xsn-internal-dns interface ethernet1/2 set network dns-proxy proxy-xsn-internal-dns enabled yes</pre>



Démo





Firewall Troubleshooting

Découvrir les sessions et les états



Mohamed Anass EDDIK

Une formation
Alphorm.com



Firewall Troubleshooting

Plan

C'est quoi une session ?
Les états de la session

Une formation
Alphorm.com

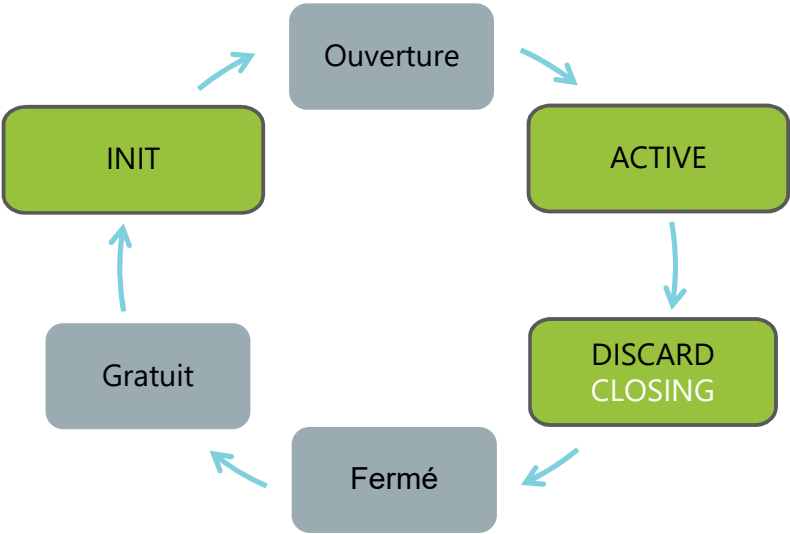
C'est quoi une session ?

Une session est un ensemble de deux flux de données unidirectionnels entre un client (initiateur) et un serveur (répondeur)

TCP	UDP	Other
• Des SYN-ACK aux FIN-ACK • Peut être réinitialisé (RST) ou chronométré à la place • La même chose qu'une "connexion" TCP	• Du premier paquet vu à la perte de 30 secondes du paquet précédent • Pas d'"état", donc pas de "fin" certaine • Limité (artificiellement) par une minuterie de rafraîchissement	• Semblable à UDP pour d'autres protocoles IP sans connexion • Aucune session pour les protocoles non IP, qui ne sont pas abandonnés, sur la base de la politique



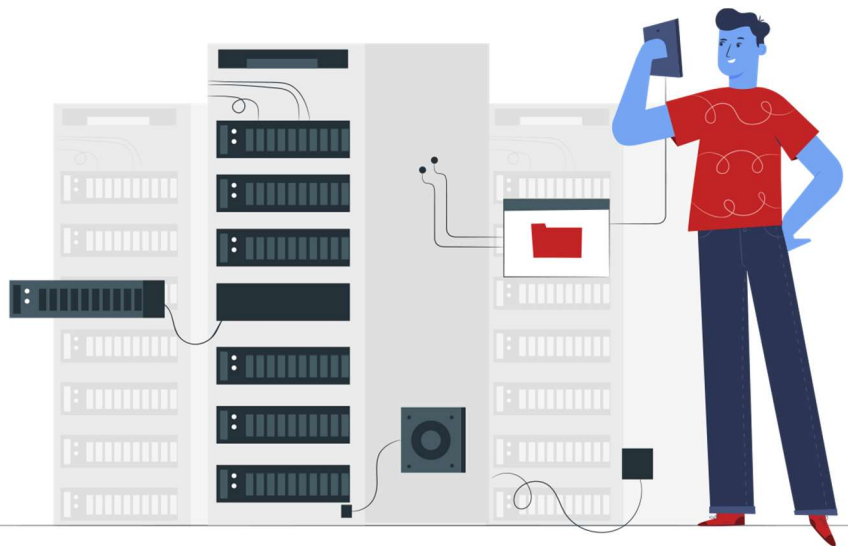
Les états de la session





Firewall Troubleshooting

Démo



Une formation
Alphorm.com



Firewall Troubleshooting

Etudier la logique des flux



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

- Diagnostic Hardware
- Diagnostic Software
- Flux de paquets Data-Plane

Une formation
Alphorm.com

Diagnostic Hardware

Key Term	Alternative Names	Definition
Network processor 	- NPU - Offload processor - EZchip - FPGA - ASIC	Fournit un support matériel personnalisé (c'est-à-dire le déchargement) pour l'émulation initiale des paquets et la recherche de flux, et le transit direct de certains paquets de charge utile qui n'ont pas besoin d'inspection de la couche 7
Security Processeur 	- CPU - Data-plane processor - Cavium processor	Gère la plupart du traitement DATA-Plane sur le FW Pour les pare-feu qui n'ont pas de processeur réseau, le processeur de sécurité gère tout le traitement du réseau.
Hardware offload 	- Offload - Session offload	Deux types possibles de déchargement matériel sont sur les pare-feu Palo Alto Networks: déchargement du réseau et le chargement de modèle-match. Le déchargement de type-match est utilisé par les processus App-ID et Content-ID. "Session déchargement" se réfère toujours au déchargement du réseau.

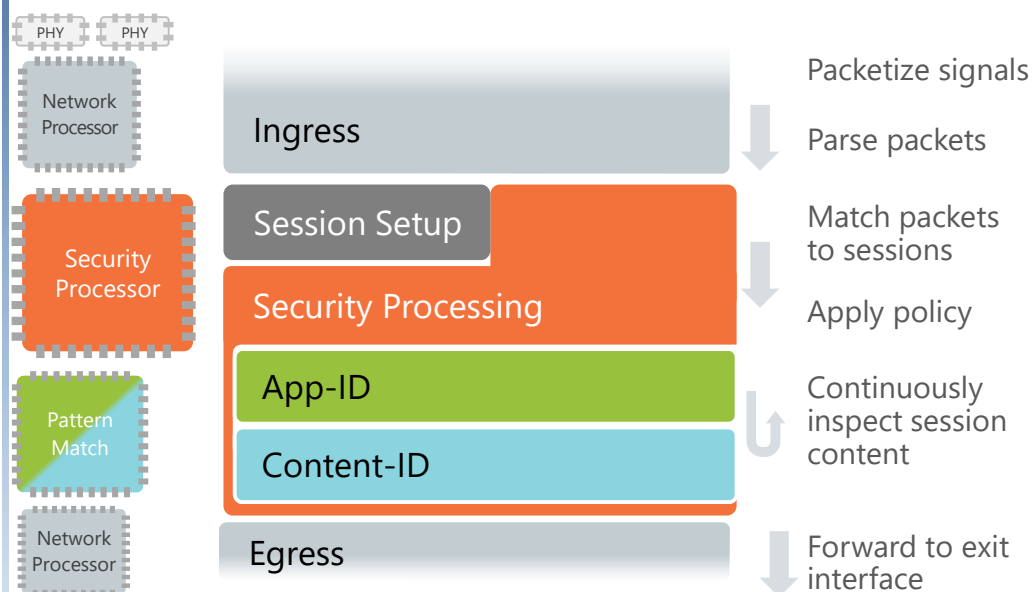
Diagnostic Software

Key Term	Alternative Names	Definition
Security processing 	- Firewall processing - CPU processing	Fournit le traitement De base L2-L4, NAT, App-ID et Content-ID signature matching, détection de la menace, évaluation du décryptage SSL, et d'autres inspections de contenu couche 7
App-ID 	Application identification	Identification d'application basée sur le contenu. Les types d'applications peuvent être détectés par le moteur App-ID lui-même et par une inspection ultérieure du contenu.
Content-ID 	- Content inspection - Layer 7 processing - Threat detection	Inclut l'antivirus, l'anti-spyware, la protection des vulnérabilités, le filtrage d'URL, le blocage de fichiers, la soumission ® WildFire, le filtrage des données et la protection DoS
Session offload	Offload	La fonction logicielle qui signale les sessions de déchargement vers un processeur réseau



Flux de paquets Data-Plane

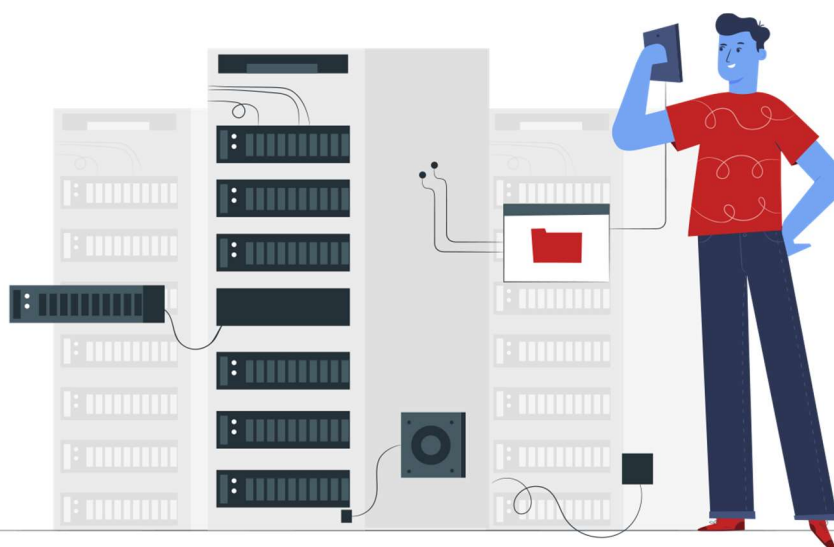
Une formation
Alphorm.com





Firewall Troubleshooting

Démo



Une formation
Alphorm.com



Firewall Troubleshooting

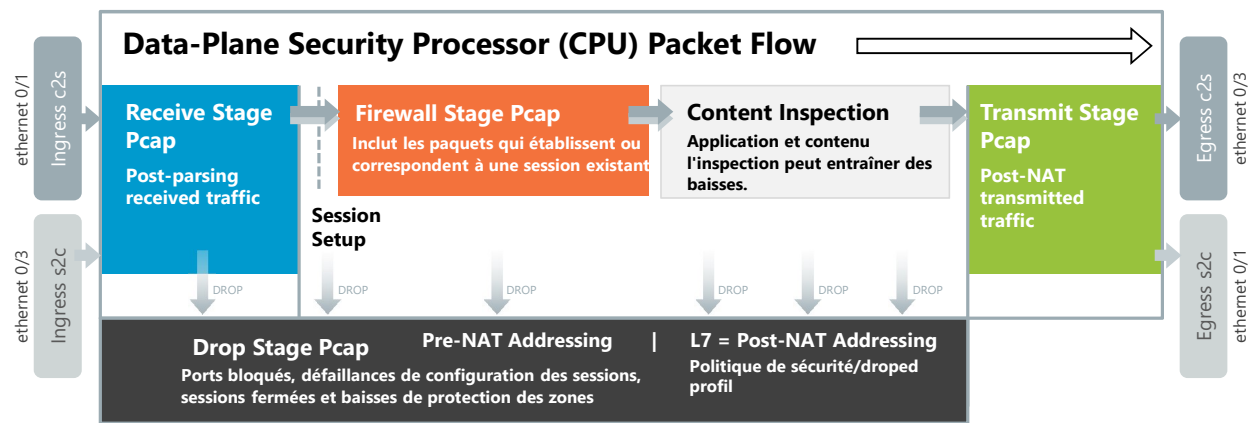
Connaître la capture des paquets



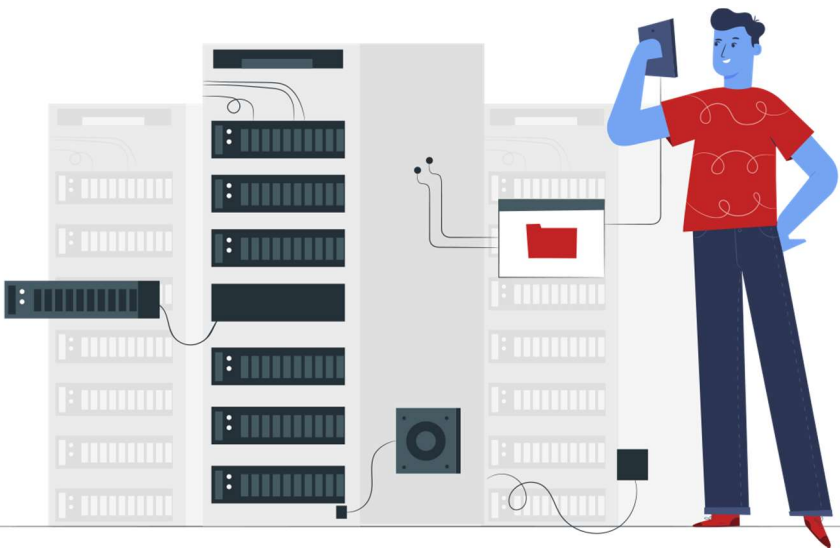
Mohamed Anass EDDIK

Une formation
Alphorm.com

Étapes de capture de paquets



Démo





Firewall Troubleshooting

Configurer la capture des paquets



Mohamed Anass EDDIK

Une formation
Alphorm.com



Firewall Troubleshooting

Connaitre les caractéristiques des logs du débogage



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

Le périmètre du flow-basic log
Les étapes pour utiliser Flow
Basic

Une formation
Alphorm
com



Le périmètre du flow-basic log

Aucune information L7 :

Enregistre la politique L7 sur le premier paquet uniquement

Pas de véritable App-ID

Pas d'URL HTTP get

Pas de SSL handshake

Aucune trace d'interception proxy SSL

Une formation
Alphorm
com



Firewall Troubleshooting

Une formation
Alphorm.com

Les étapes pour utiliser Flow Basic

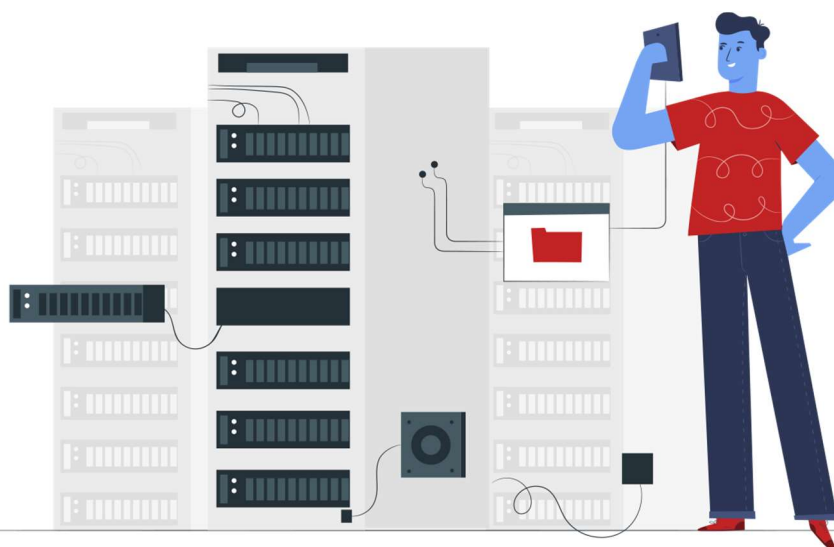
- Effacer les anciens paramètres
- Filtrer de façon étroite (et tester)
- Configurer les étapes de capture
- Activer le flux de base
- Vérifier les sessions en cours
- Activer la capture puis l'enregistrement
- Capture de moniteur
- Désactiver l'enregistrement puis capturer
- Afficher les logs de base du flux
- Afficher les pcaps



Firewall Troubleshooting

Une formation
Alphorm.com

Démo





Firewall Troubleshooting

Une formation
Alphorm.com

Interpréter les flux des logs générés



Mohamed Anass EDDIK



Firewall Troubleshooting

Une formation
Alphorm.com

Etapes

Vérifier que les paquets sont vus

Tracer les flux de paquets à travers le pare-feu :

- Vérifier la configuration de la session et le trafic de retour

- Vérifier la configuration de la session «**Predict**» (le cas échéant)

- Comparer les temps d'entrée et d'évacuation

Vérifier les correspondances de la politique L2-L4 en corrélation avec :

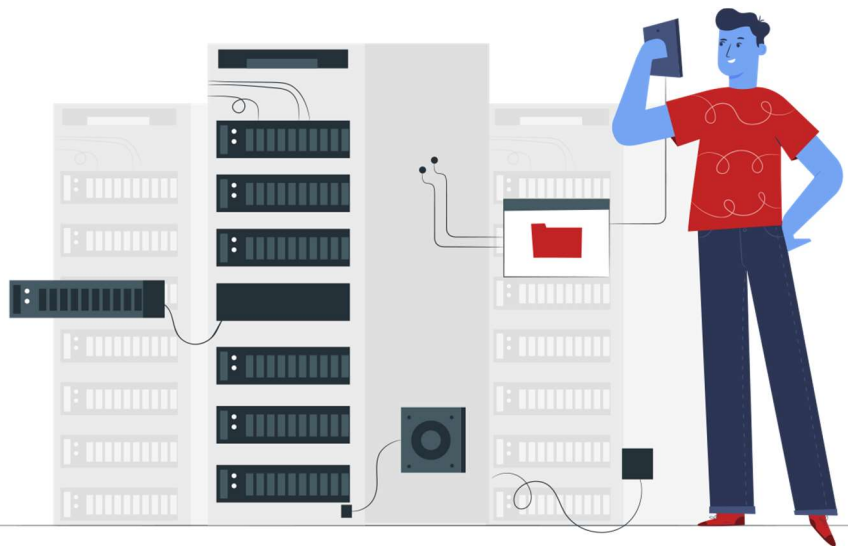
- Pcaps** avec informations sur la couche d'application

- Autres données du journal



Firewall Troubleshooting

Démo



Une formation
Alphorm.com



Firewall Troubleshooting

Assurer l'assistance matérielle et déchargement



Mohamed Anass EDDIK

Une formation
Alphorm.com



Une formation
Alphorm.com

Plan

Déchargement matériel vers
le processeur réseau
Quel trafic peut être
déchargé?



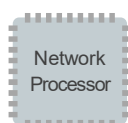
Une formation
Alphorm.com

Déchargement matériel vers le processeur réseau

Session-match, route, and ARP lookups

NAT, le cas échéant (sur les paquets déchargés seulement)

Gestion de file d'attente QoS, le cas échéant





Firewall Troubleshooting

Une formation
Alphorm.com

Quel trafic peut être déchargé?

Les sessions SSL et SSH qui ne sont pas sujet de décryptage

Sessions auxquelles une règle de remplacement d'application est appliquée avec une application personnalisée

Protocoles de routage dynamiques tels que OSPF, BGP ou RIP

Sessions basées sur des protocoles pour lesquels il n'existent pas d'exploits connus, de sorte qu'une inspection supplémentaire ne s'applique pas

Ce trafic ne sera jamais déchargé :

Non-TCP/UDP (including ping)

ARP (all non-IP traffic)

NAT64

TCP SYN, FIN, and RST

Navigation sur le Web

SSL décrypté

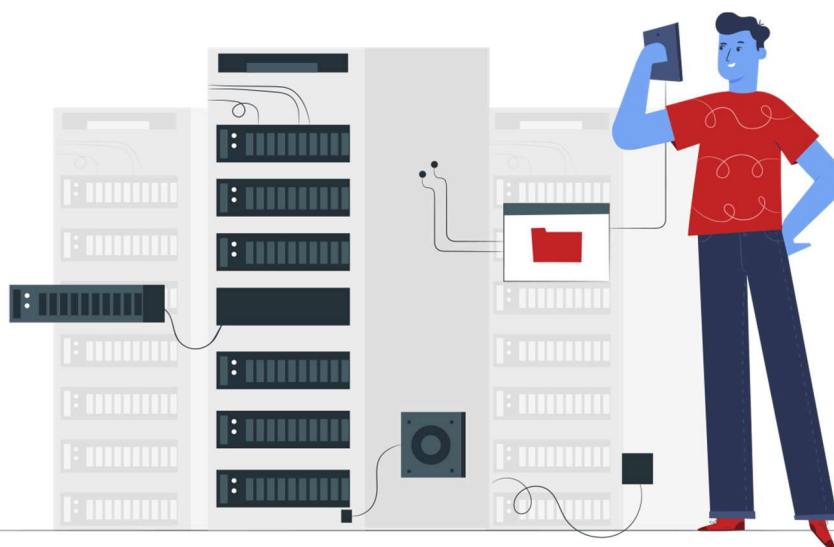
Séances liées au pare-feu



Firewall Troubleshooting

Une formation
Alphorm.com

Démo





Firewall Troubleshooting

Une formation
Alphorm.com

Identifier le type de trafic



Mohamed Anass EDDIK



Firewall Troubleshooting

Une formation
Alphorm.com

Plan

C'est quoi le trafic host-entrant ?
Progression générale pour les diagnostics spécifiques aux fonctionnalités



C'est quoi le trafic host-entrant ?

Le trafic hôte-entrant se termine sur l'interface de gestion ou les interfaces data-plane, il est traité par le pare-feu lui-même :

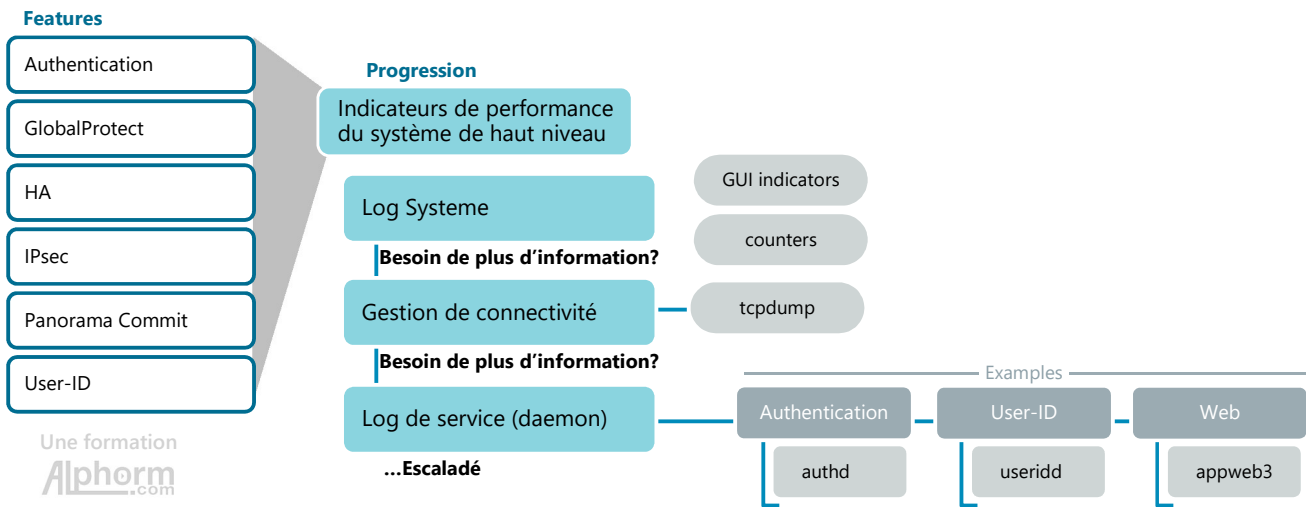
MGT interface examples :

- Management
- Ping
- SNMP
- User-ID
- Authentication
- Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL)

Data-plane examples :

- Routing protocol updates
- Ping
- GlobalProtect
- IPsec

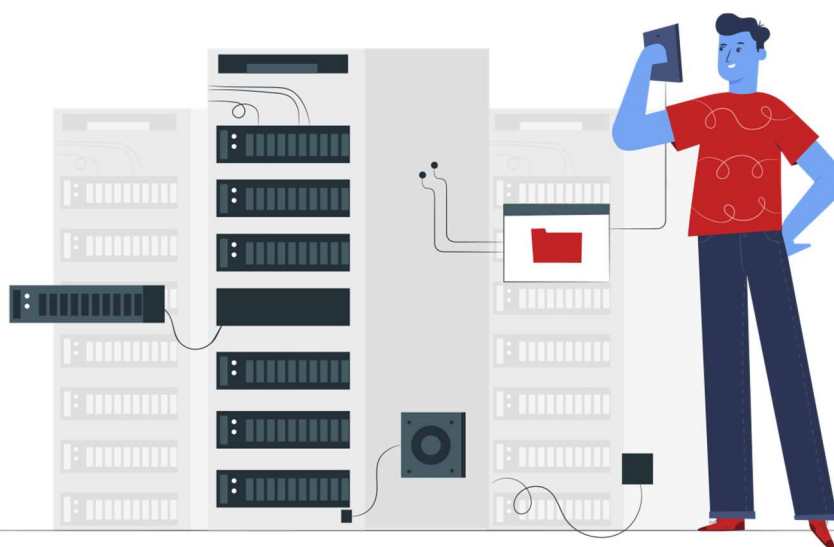
Progression générale pour les diagnostics spécifiques aux fonctionnalités





Firewall Troubleshooting

Démo



Une formation
Alphorm.com



Firewall Troubleshooting

Diagnostiquer le Traffic VPN



Mohamed Anass EDDIK

Une formation
Alphorm.com



Firewall Troubleshooting

Une formation
Alphorm.com

Plan

Dépannage VPN

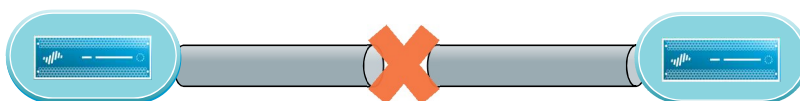
Le tunnel ne s'établit pas
Établissement du tunnel :
Contexte



Firewall Troubleshooting

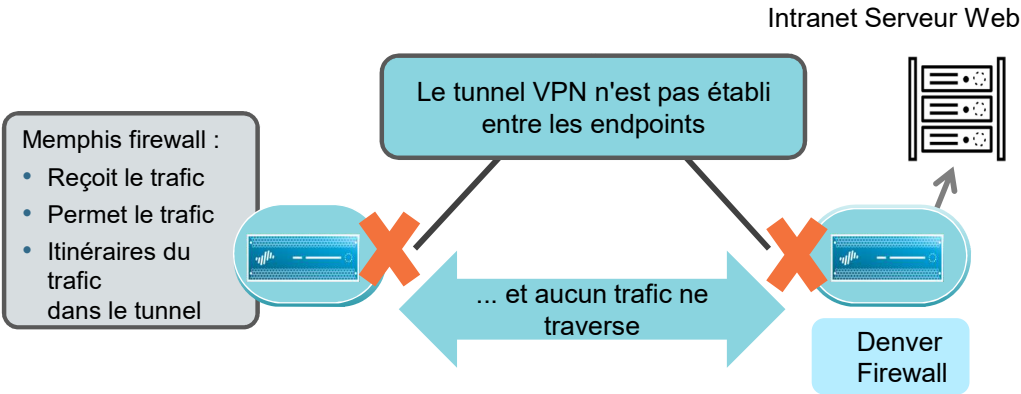
Une formation
Alphorm.com

Dépannage VPN

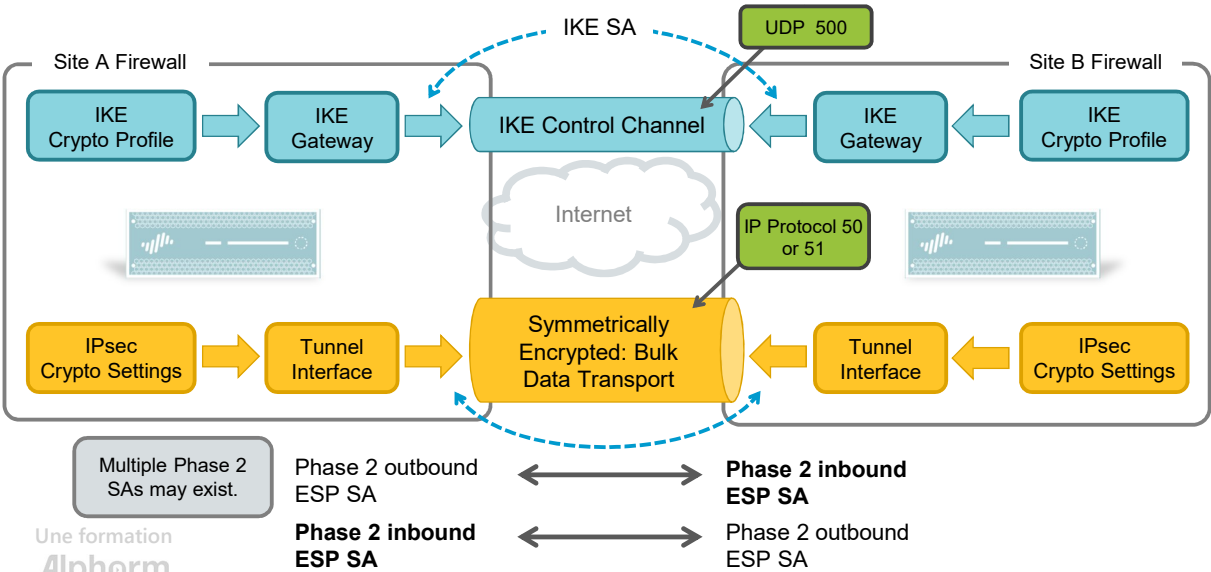




Le tunnel ne s'établit pas



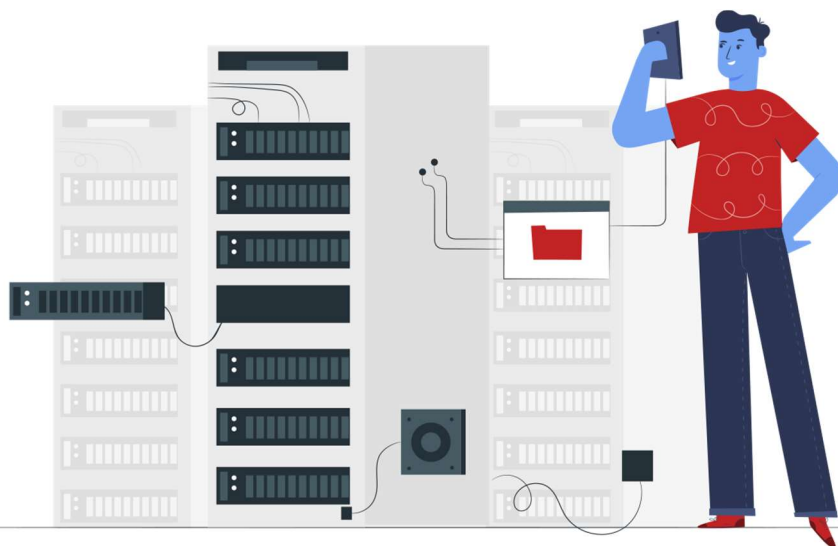
Établissement du tunnel : Contexte





Firewall Troubleshooting

Démo



Une formation
Alphorm.com



Firewall Troubleshooting

Diagnostiquer l'IKE



Mohamed Anass EDDIK

Une formation
Alphorm.com



Firewall Troubleshooting

Une formation
Alphorm.com

Vérifier le Management Interface



Mohamed Anass EDDIK



Firewall Troubleshooting

Une formation
Alphorm.com

Connaitre le type de trafic



Mohamed Anass EDDIK



Plan

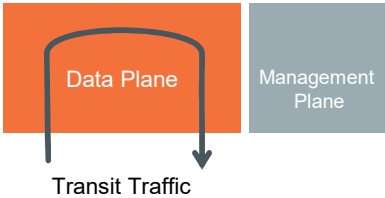
C'est quoi le Transit Traffic? Troubleshooting Progression

Une formation
Alphorm.com

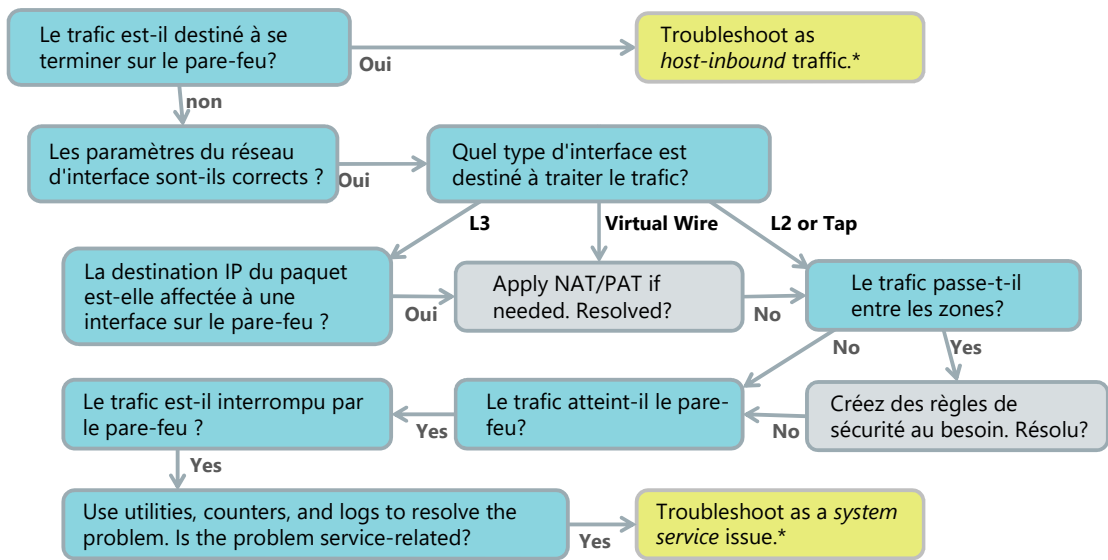
C'est quoi le Transit Traffic?

Transit Traffic passe à travers le pare-feu
Trafic acheminé entre deux interfaces de data plane

Reçu sur le data-plane	Transféré
interface physique	out physical interface
sous-interface	out subinterface
interface physique	to loopback interface
physical interface	à l'interface tunnel, puis à l'extérieur



Troubleshooting Progression



Démo





Firewall Troubleshooting

Une formation
Alphorm.com

Collecter les informations



Mohamed Anass EDDIK



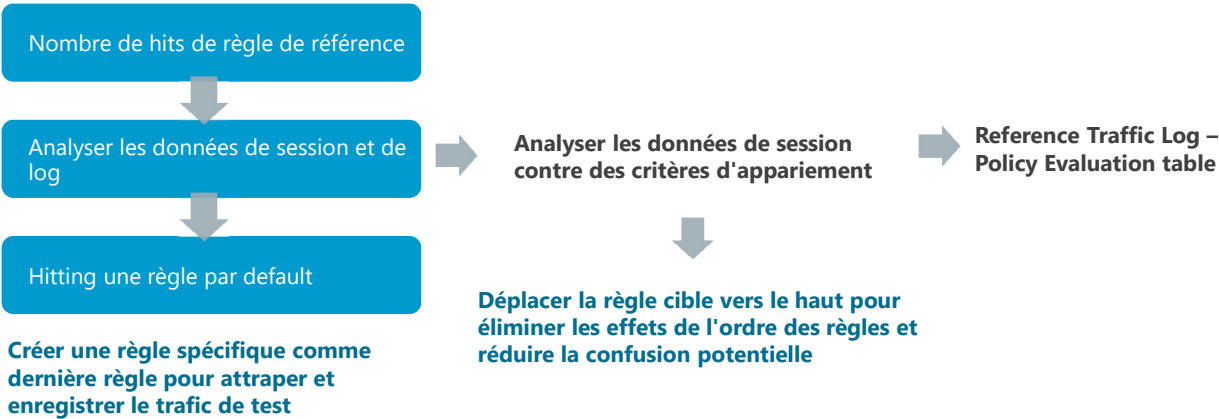
Firewall Troubleshooting

Une formation
Alphorm.com

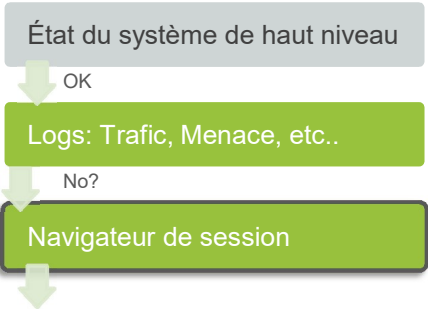
Plan

Dépannage Rule-Match
Avoir des sessions, mais pas
de log

Dépannage Rule-Match



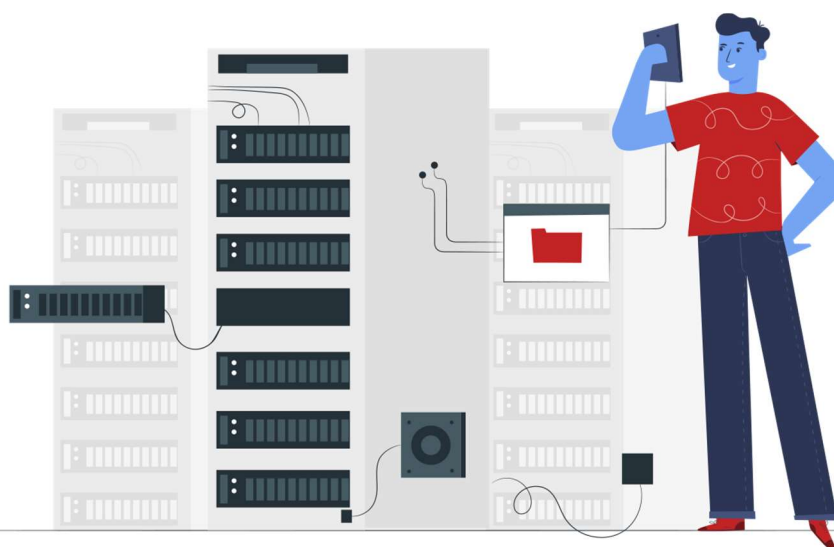
Avoir des sessions, mais pas de log





Firewall Troubleshooting

Démo



Une formation
Alphorm.com



Firewall Troubleshooting

Utiliser les counters



Mohamed Anass EDDIK

Une formation
Alphorm.com

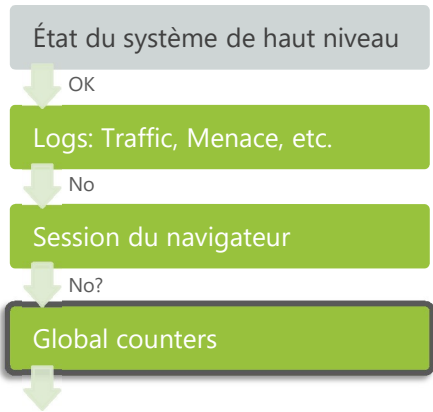


Plan

Recevoir du trafic mais aucune session
Besoin d'une preuve de trafic ou plus
d'info

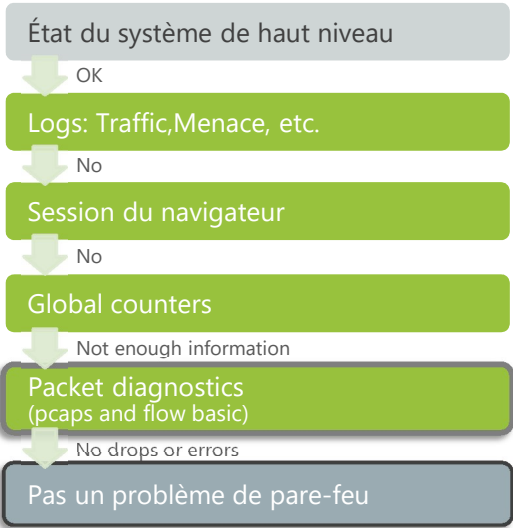


Recevoir du trafic mais aucune session

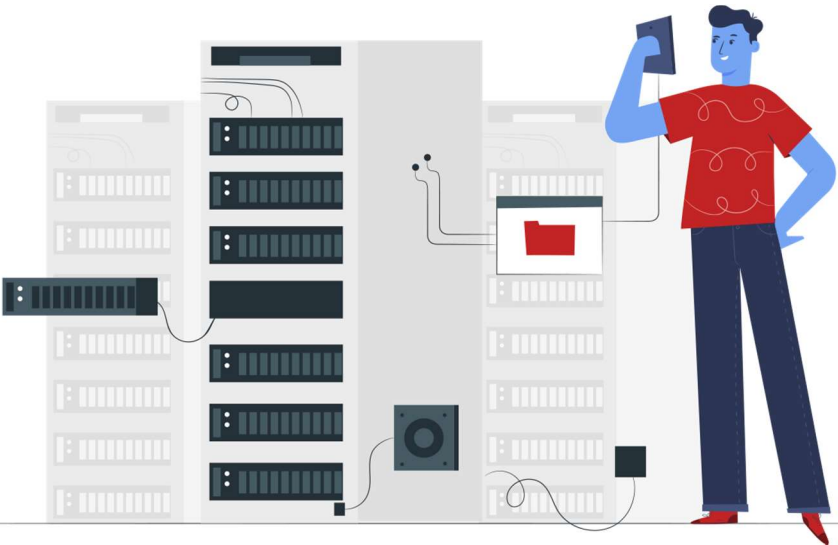




Besoin d'une preuve de trafic ou plus d'info



Démo





Identifier les problèmes de performance



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

C'est quoi les problèmes des performances?

Progression de dépannage de performance

Une formation
Alphorm.com

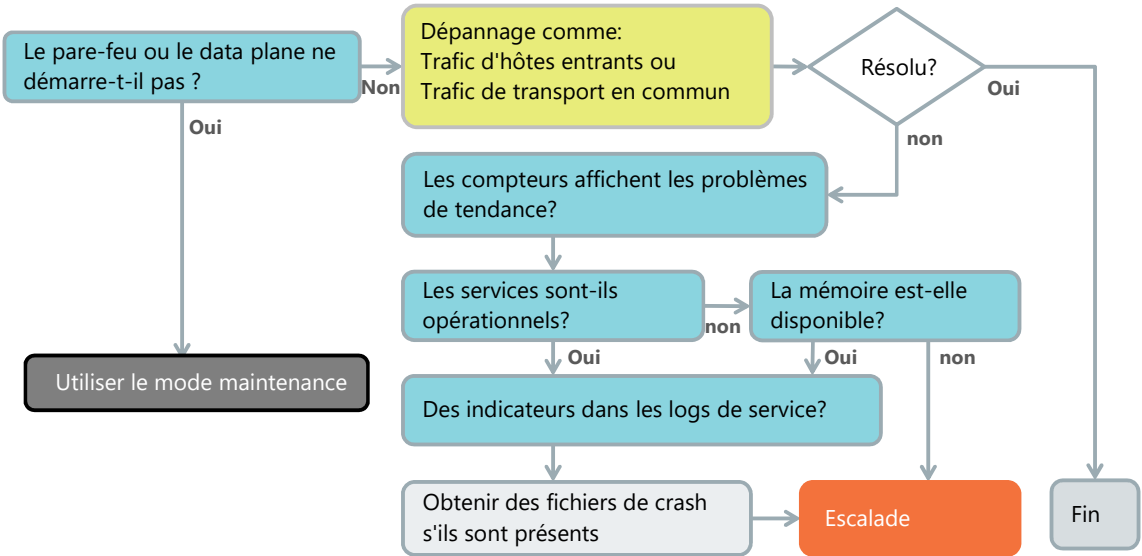


C'est quoi les problèmes des performances?

Les problèmes de performances sont des problèmes de système avec management plane et le data plane :

- Défaillances de service
- Échecs d'allocation des ressources
- Échecs de validation
- Échecs de mise à jour

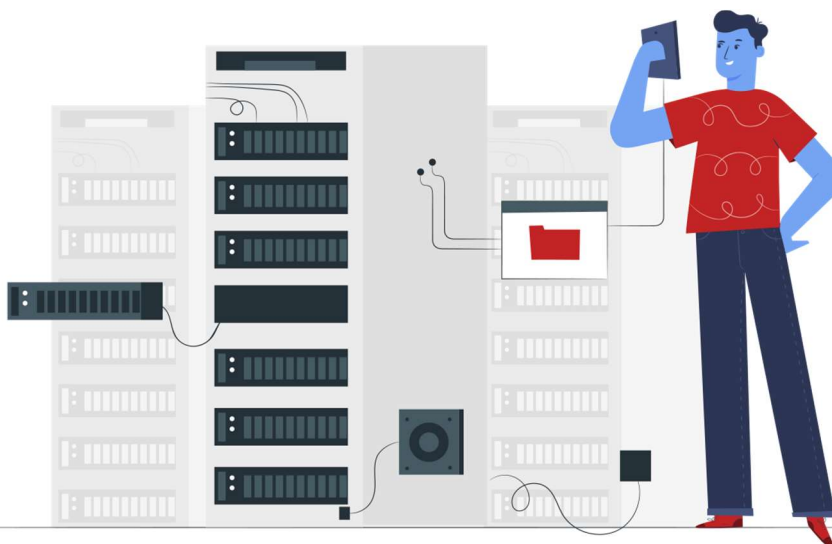
Progression de dépannage de performance





Firewall Troubleshooting

Démo



Une formation
Alphorm.com



Firewall Troubleshooting

Voir un aperçu des services système



Mohamed Anass EDDIK

Une formation
Alphorm.com



Une formation
Alphorm.com

Plan

Services Système (Daemons)
Quelques services mangement
plane



Une formation
Alphorm.com

Services Système (Daemons)

Core PAN-OS® management-plane and
data-plane functions :

- Sont mis en œuvre dans des logiciels individuels appelés Daemons
- Comprennent plus de 100 services individuels (daemons)
- Incluent de nombreux services qui écrivent leurs propres journaux



Firewall Troubleshooting

Une formation
Alphorm.com

Services Système (Daemons)

Service (daemon) logs :

- Peut fournir des informations précieuses pour le dépannage
- Peut inclure une propriété de niveau journal de débogage qui définit le type d'événements enregistrés
- Peut être affiché localement dans le CLI
- Peut être exporté pour l'analyse à distance

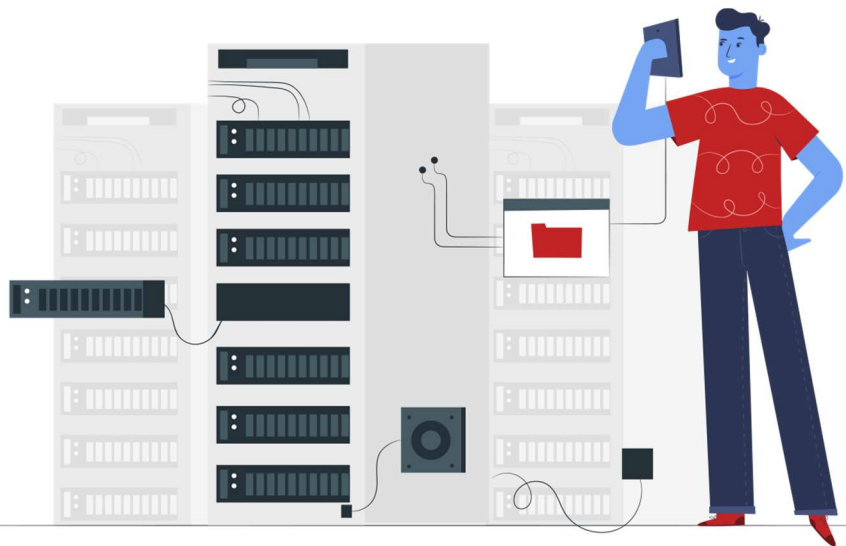
Quelques services mangement plane

	Process/Daemon	Description	Log Name
Opérations internes	management-server	Met en œuvre des services de gestion backend; gère la gestion de la configuration, les opérations de validation, les rapports, etc. (runs as "mgmtsrvr")	ms.log
	device-server	Pousse les configurations vers le plan de données et gère diverses communications avec le plan de données, telles que les recherches d'URL	devsrvr.log
Externe	high-availability	Gère l'état de haute disponibilité, la synchronisation de configuration, etc.	ha-agent.log
	routing	Fournit des services de routage et de routage dynamique de l'état-machine	routed.log
Logs	log-receiver	Enregistre les logs de trafic envoyés à partir de la data plane	logrcvr.log
	syslog-ng	Handles log forwarding	syslog-ng.log
	vardata-receiver	Enregistre les les d'URL et les pcaps envoyés à partir du data plane	varrcvr.log



Firewall Troubleshooting

Démo



Une formation
Alphorm.com



Firewall Troubleshooting

Collecter plus de données



Mohamed Anass EDDIK

Une formation
Alphorm.com



Diagnostiquer le décryptage SSL

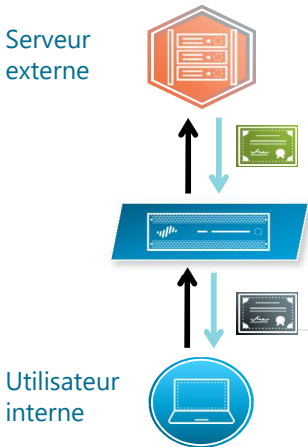


Mohamed Anass EDDIK

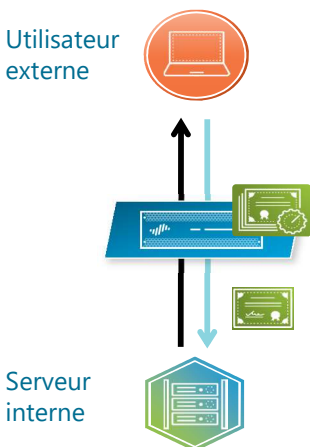
Une formation
Alphorm.com

Types de règles de stratégie de décryptage

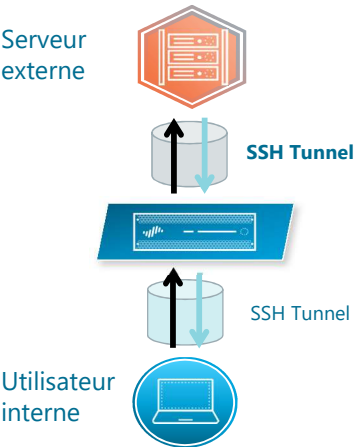
Proxy SSL Forward (sortant)



SSL Inbound Inspection



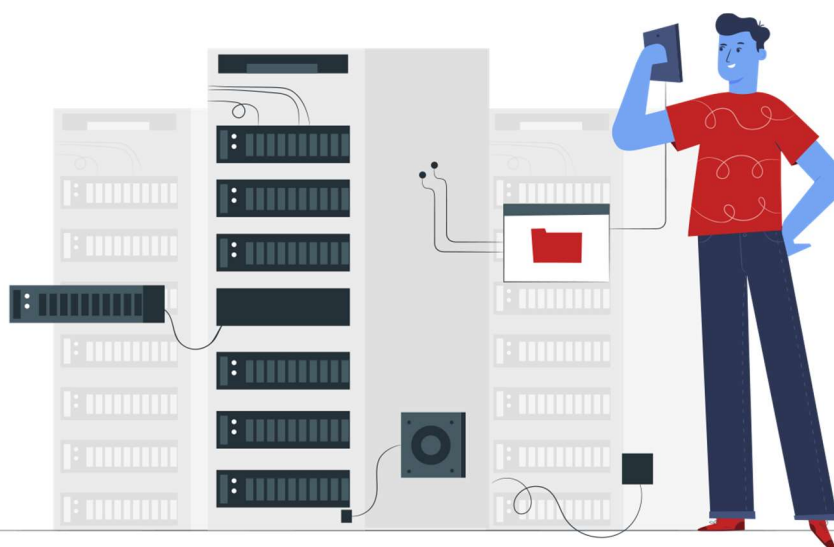
SSH Proxy





Firewall Troubleshooting

Démo



Une formation
Alphorm.com



Firewall Troubleshooting

Gérer les facteurs externes pour le décryptage SSL



Mohamed Anass EDDIK

Une formation
Alphorm.com



Firewall Troubleshooting

Plan

Épinglage de certificat (HPKP) Application ECDHE et impact sur la sécurité

Une formation
Alphorm.com



Firewall Troubleshooting

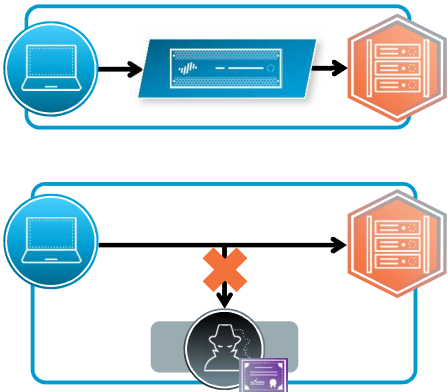
Épinglage de certificat (HPKP)



Une formation
Alphorm.com



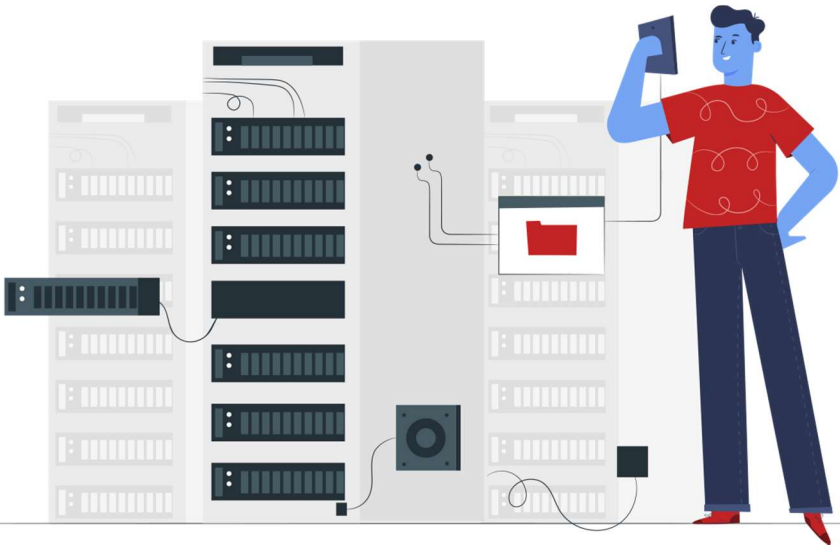
Application ECDHE et impact sur la sécurité



Une formation
Alphorm.com



Démo



Une formation
Alphorm.com



Firewall Troubleshooting

Détailler le flux de mappage des User-ID



Mohamed Anass EDDIK

Une formation
Alphorm.com



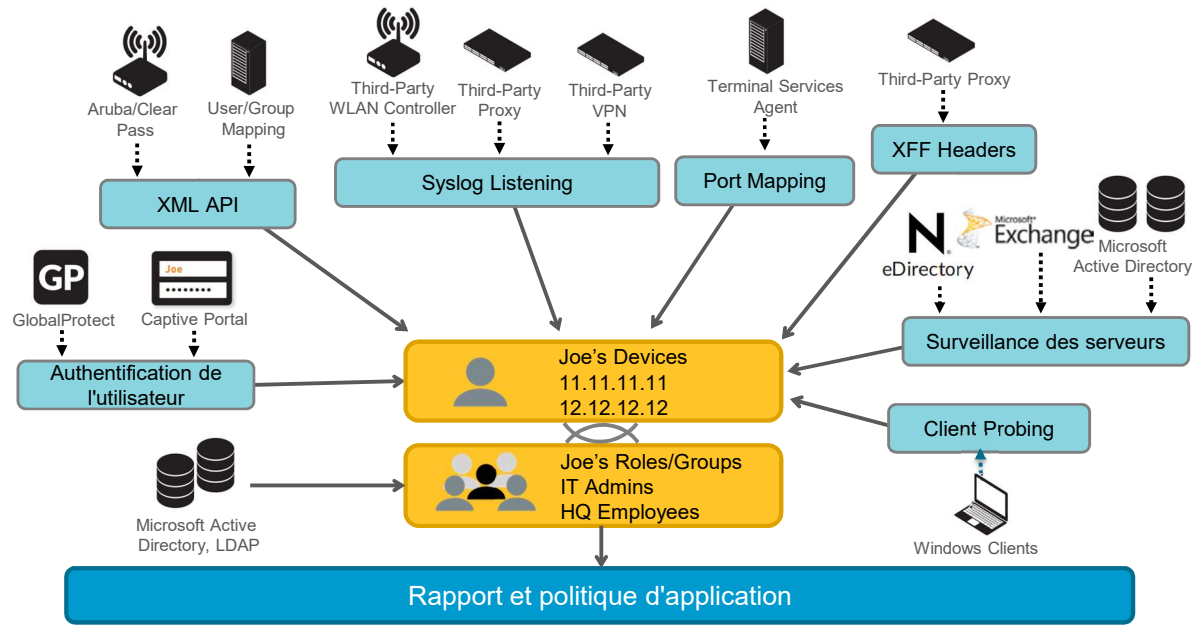
Firewall Troubleshooting

Plan

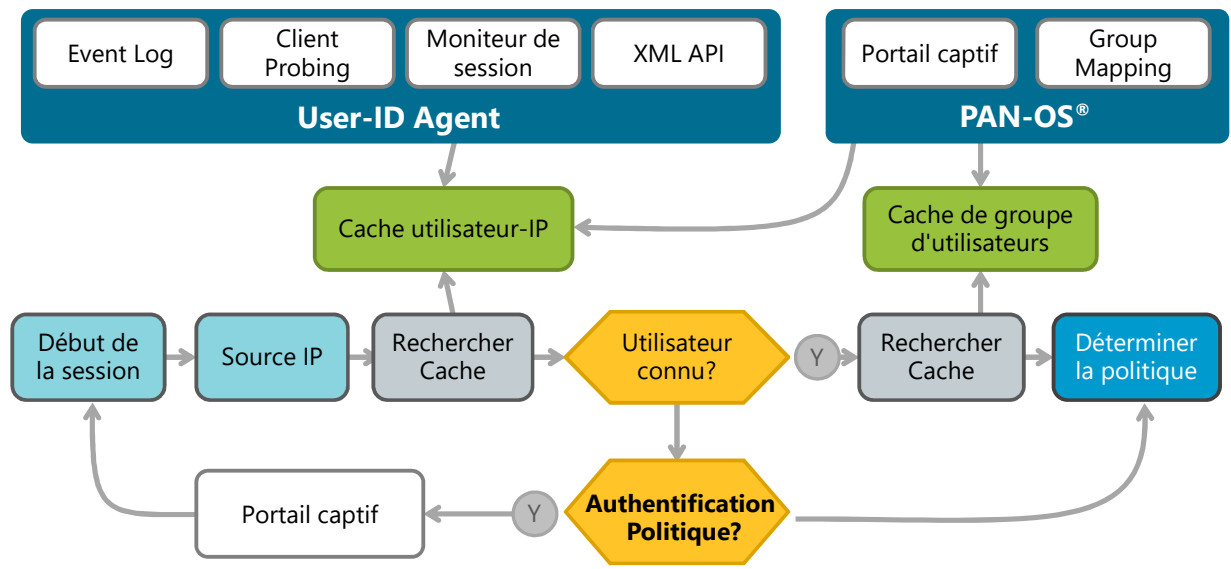
Méthodes du mapping des utilisateurs
Flux d'agent User-ID

Une formation
Alphorm.com

Méthodes du mapping des utilisateurs



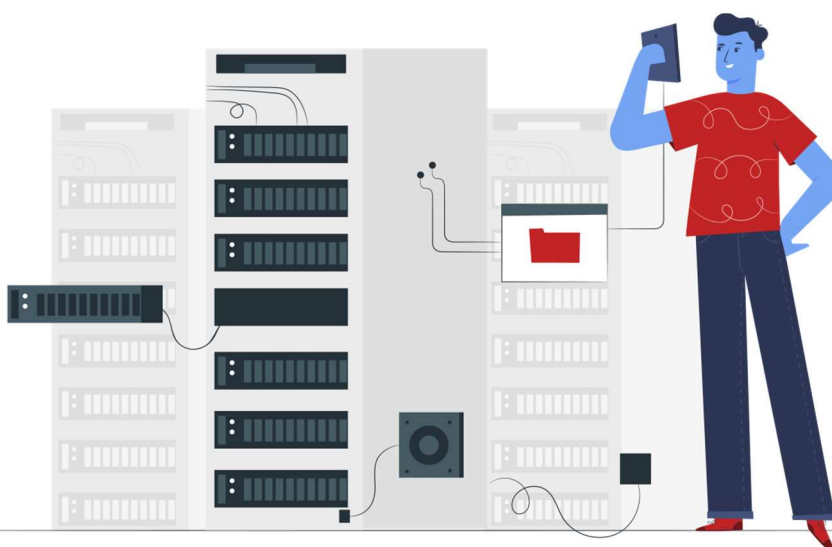
Flux d'agent User-ID





Firewall Troubleshooting

Démo



Une formation
Alphorm.com



Firewall Troubleshooting

Débloquer le User-ID agent



Mohamed Anass EDDIK

Une formation
Alphorm.com

Exigences pour l'extraction d'informations sur les serveurs

Création d'un compte de service dédié

Affectation des membres du groupe suivants :

Lecteurs de journaux d'événements : Lire le journal des événements de sécurité

Opérateurs de serveurs (facultatif) : Actualiser les cartographies en surveillant les sessions utilisateur

Les événements enregistrés sur le serveur doivent être des événements d'authentification réussis :

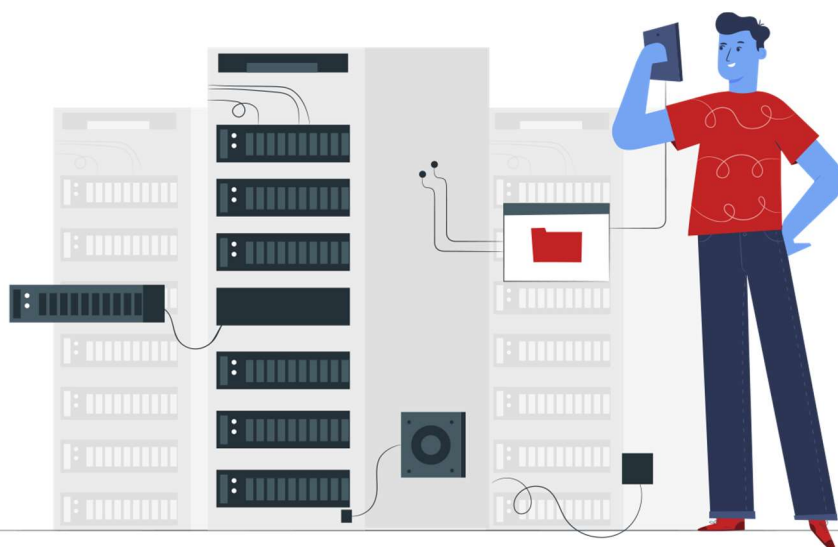
Ouvrir les sessions de serveur

Avec plusieurs serveurs, on doit identifier le serveur dont l'utilisateur est authentifié (serveur de connexion echo)



Démo

Une formation
Alphorm.com





Firewall Troubleshooting

Diagnostiquer les users et les groups mapping



Mohamed Anass EDDIK

Une formation
Alphorm.com



Firewall Troubleshooting

Vérifier l'authentification



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

Liste de contrôle de configuration
Authentication Policy Troubleshooting
Progression
Étapes de dépannage User-ID

Une formation
Alphorm.com

Liste de contrôle de configuration

Activer l'USER-ID sur la zone source : Configurer une liste de contrôle d'accès dans la zone

Activer la politique d'authentification

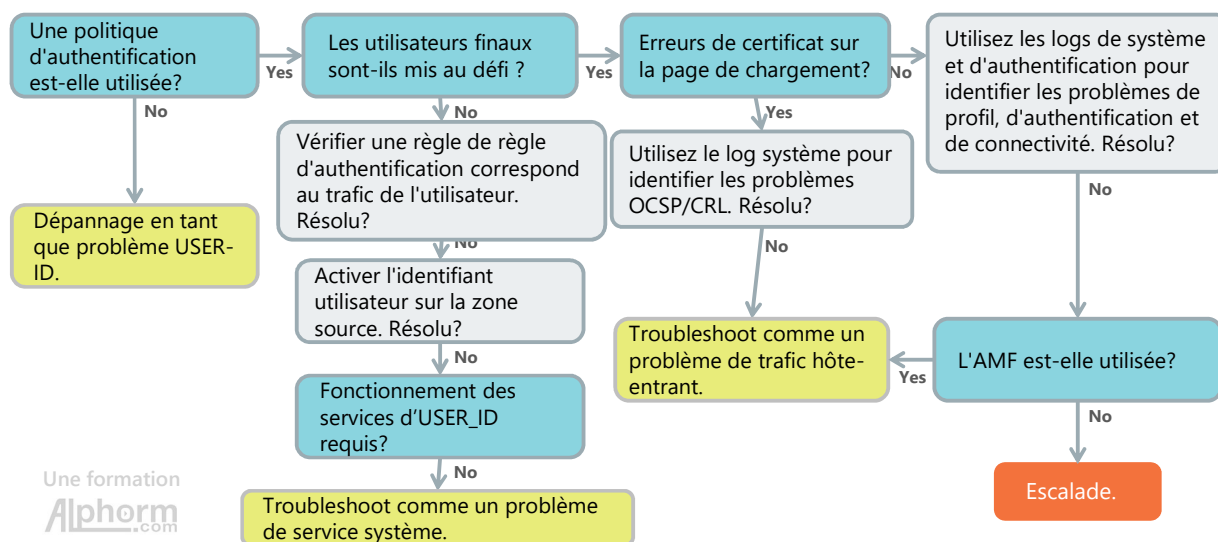
Configurer les paramètres de la stratégie d'authentification de l'identification des utilisateurs

Définir la règle de la politique d'authentification pour être défi de navigateur ou formulaire Web

Activer un profil de gestion pour une interface de page de réponse

Créer des règles de politique de sécurité au besoin

Authentication Policy Troubleshooting Progression



Liste de contrôle de configuration

Inspectez les journaux du système et de l'authentification

Utilisez la commande de test pour trouver la correspondance de la stratégie d'authentification

Vérifiez que les défis sont reçus; les utilisateurs obtiennent-ils le formulaire Web ?

Filtrez les compteurs globaux par adresse IP source

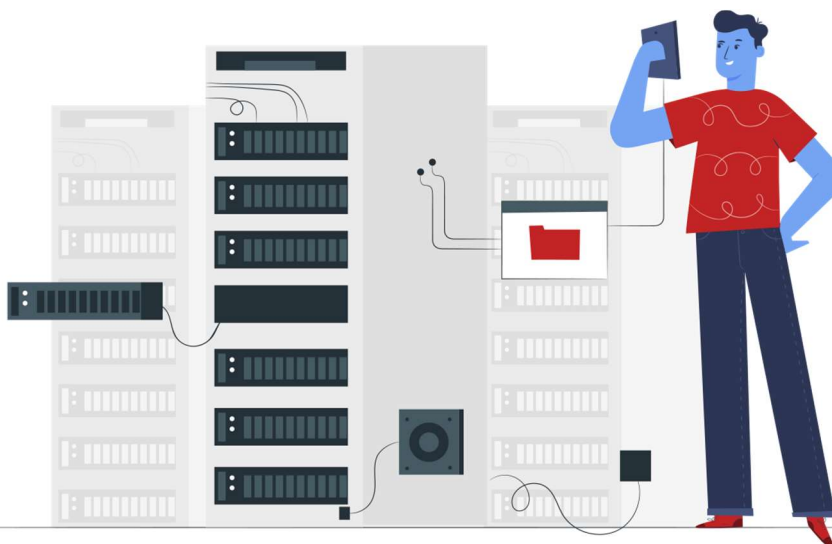
Activez le débogage sur les services L3 (NTLM) et l'Utilisateur-ID (l3svc et user-id) et exécutez l'agent de débogage de l'identifiant utilisateur ntlm

En l'absence d'erreurs, cochez le décryptage : activé ou non ?



Firewall Troubleshooting

Démo



Une formation
Alphorm.com



Firewall Troubleshooting

Découvrir les problèmes courants de GlobalProtect



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

GlobalProtect Troubleshooting GlobalProtect Progression

Une formation
Alphorm.com



GlobalProtect Troubleshooting

Pour l'initialisation et l'établissement des tunnels :

- Log système et compteurs de trafic
- Capture de paquets par CLI



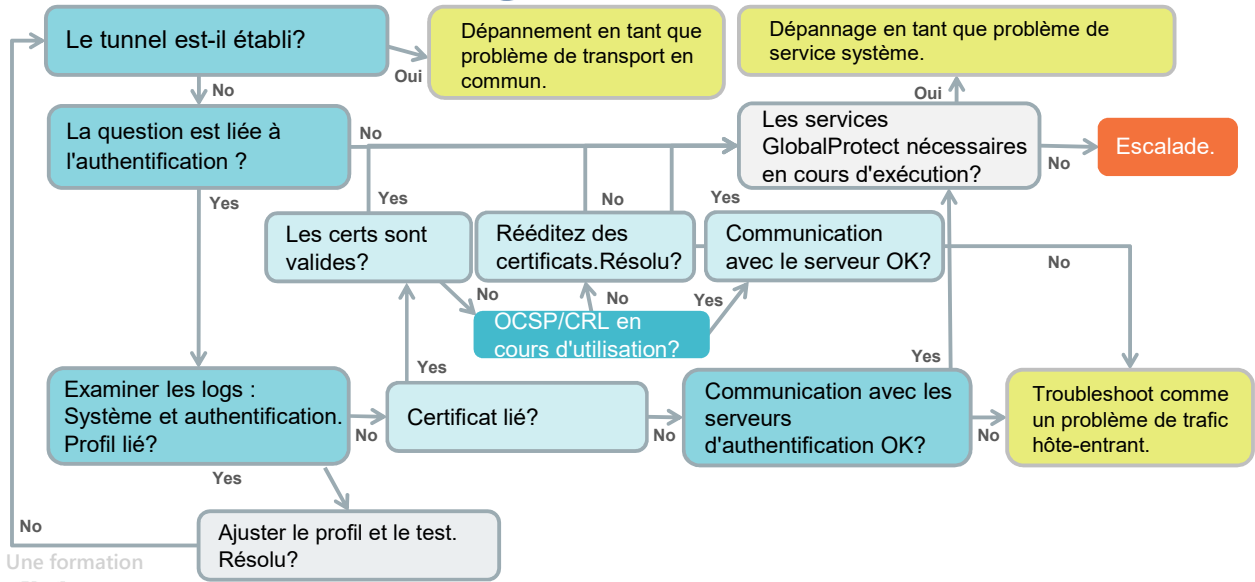
Pour l'absence de trafic dans un tunnel établi :

- Traffic logs
- Routing tables
- Traffic packet captures
- HIP logs

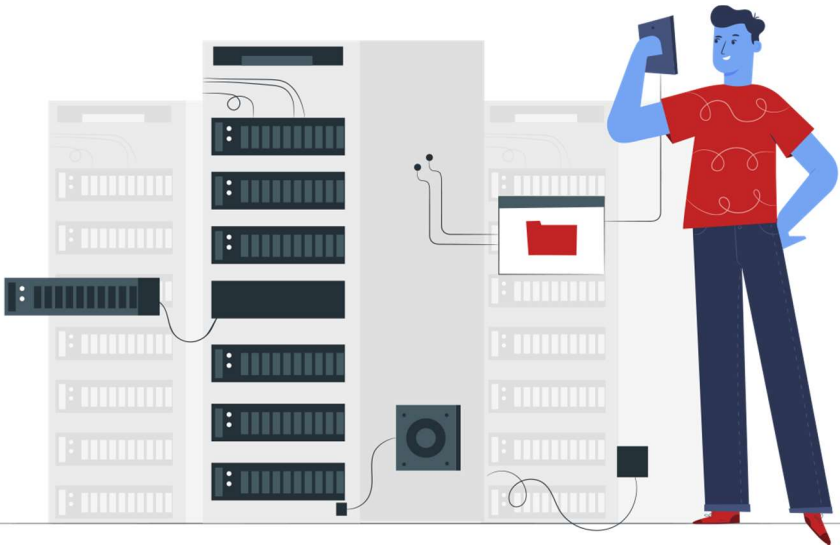


Une formation
Alphorm.com

GlobalProtect Progression



Démo





Firewall Troubleshooting

Une formation
Alphorm.com

Vérifier les logs de GlobalProtect et les certificats



Mohamed Anass EDDIK



Firewall Troubleshooting

Une formation
Alphorm.com

Plan

Configuration Checklist
GlobalProtect Agent Log
Collection



Une formation
Alphorm.com

Configuration Checklist

Licenses

Interface setup

Certificates

Client Certificate Profile

User authentication

GlobalProtect Profile

GlobalProtect Gateway Profile (passerelle externe et interne)

Host Information Profile (du client)

Créez un objet HIP ou un profil HIP et incluez-vous dans la configuration de la passerelle

Configurez les règles de sécurité appropriées avec les profils HIP



Une formation
Alphorm.com

GlobalProtect Agent Log Collection

- Main components:

- PanGPA.exe (agent UI)
- PanGPS.exe (Windows service)
- PanGPUUpdater.exe (Service Windows pour la mise à niveau et la déclassement des logiciels clients sans l'autorisation de l'administrateur)

- Log files:

- PanGPS.log (situé dans le répertoire de l'installation)
- PanGPA.log (situé dans l'annuaire par défaut de l'utilisateur)

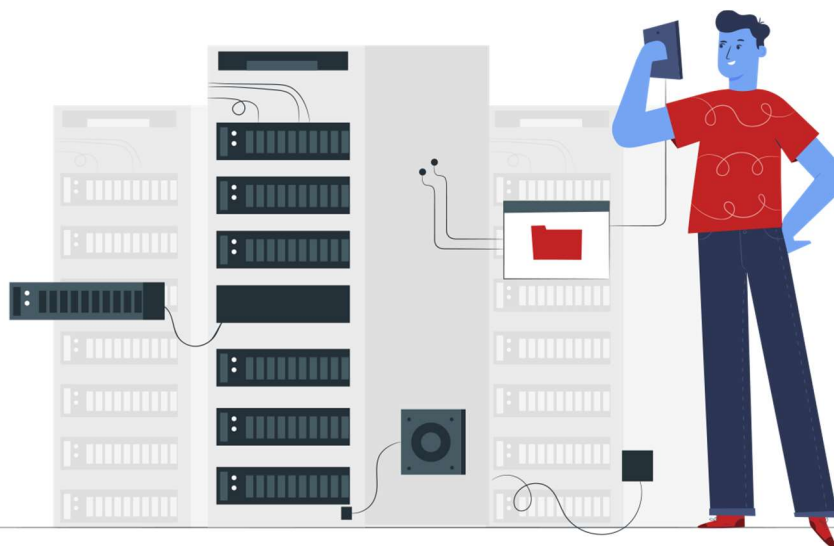
- Enable debug trace:

- Cliquez sur l'onglet Dépannage et sélectionnez Les logs.
- Ajustez le niveau de débogage pour contrôler le niveau de détail



Firewall Troubleshooting

Démo



Une formation
Alphorm.com



Firewall Troubleshooting

Conclusion



Mohamed Anass EDDIK

Une formation
Alphorm.com



Firewall Troubleshooting

Une formation
Alphorm.com

Bilan

Connaitre les outils, ressources et CLI
Comprendre le comportement des flux
Définir la capture des paquets
Diagnostiquer les paquets
Gérer le trafic des hotes-entrants
Identifier le Transit Traffic
Diagnostiquer les services Systèmes
Gérer les certificats et le décryptage SSL
Diagnostiquer les User-ID
Diagnostiquer GlobalProtect



Firewall Troubleshooting

Une formation
Alphorm.com

Cursus Palo Alto Networks



