



Formation

SOPHOS XG Firewall

Niveau Expert



Mohamed Anass EDDIK

Une formation
Alphorm.com



Cursus Sophos XG 18



Une formation
Alphorm.com



Une formation
Alphorm.com

Plan de la formation

Introduction

1. Déployer Sophos en entreprise
2. Configurer le Firewalling Avancé
3. Gérer Webserver Protection
4. Configurer le VPN pour entreprise
5. Gérer le HA et le WIFI sur un XG
6. Dépanner sur XG FW

Conclusion



Une formation
Alphorm.com

Public concerné

Support technique

Administrateur sécurité

Avant-vente sécurité

Préparer la certification Sophos XG



Prérequis

Avoir des bases en sécurité



Une formation
Alphorm.com





Une formation
Alphorm.com

Présentation du LAB de la formation



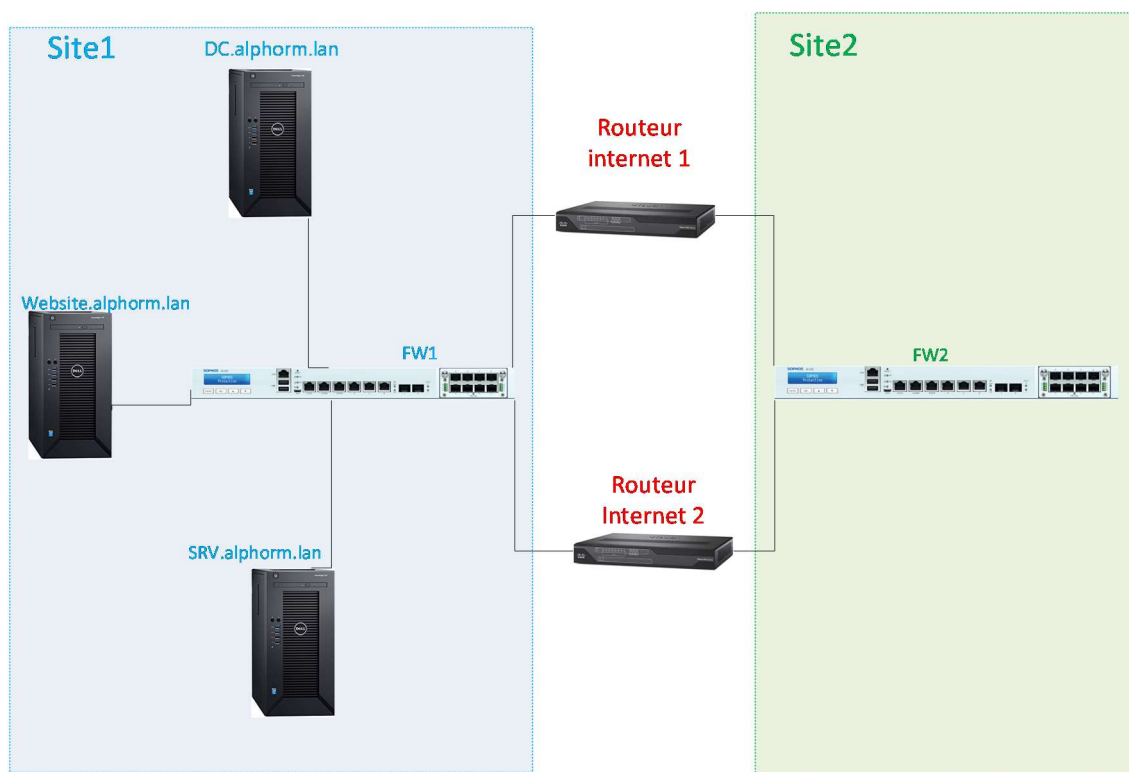
Mohamed Anass EDDIK



Une formation
Alphorm.com

Plan

Schéma du LAB
Les prérequis du Lab



Les prérequis du Lab

Une machine avec 16Go de RAM
VMware Workstation/Fusion (ou ESXi)
deux VM Sopos XG Firewall
Une marchine serveur de test



Découvrir les différents types de déploiement



Mohamed Anass EDDIK



Plan

Aperçu de types de déploiement
Gateway Mode
Bridge Mode

Une formation
Alphorm.com



Types de déploiement

Gateway mode

Bridge mode

Mixed mode

Discover mode

Une formation
Alphorm.com



Gateway Mode

Une formation
Alphorm.com

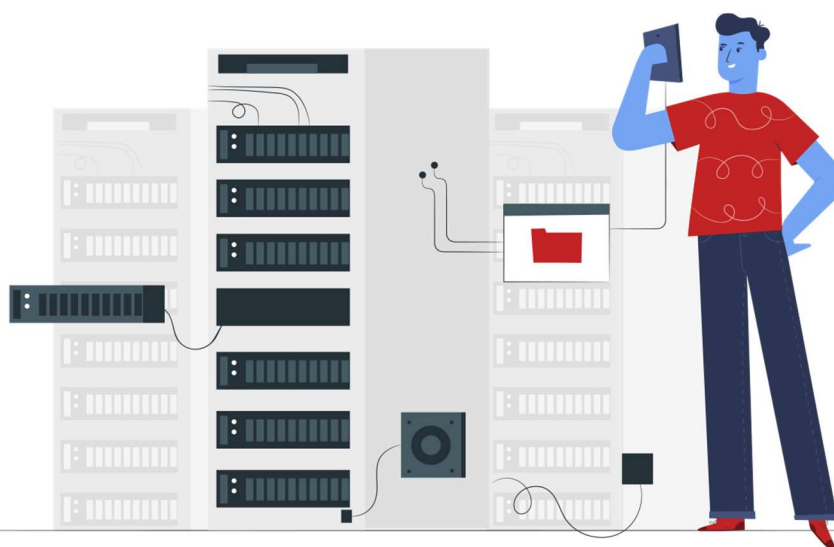


Bridge Mode

Une formation
Alphorm.com



Démo



Une formation
Alphorm.com



Découvrir les différents types de déploiement *LAB*

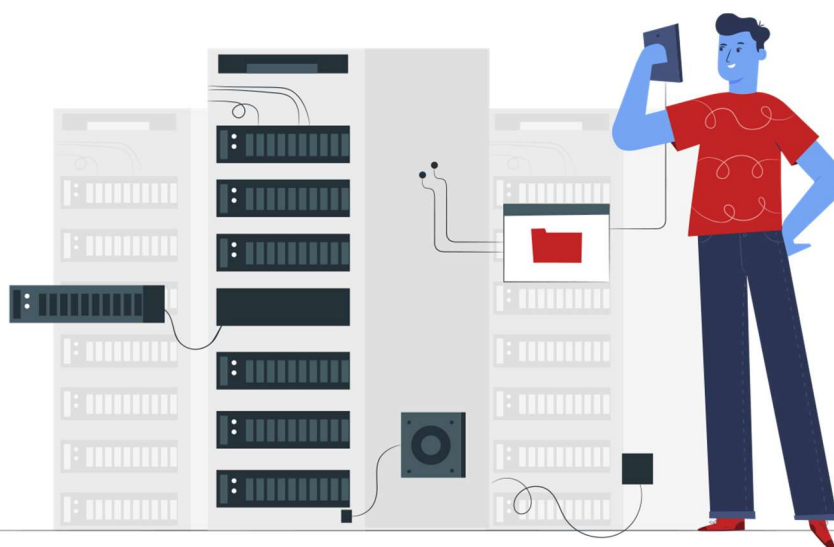


Mohamed Anass EDDIK

Une formation
Alphorm.com



Démo



Une formation
Alphorm.com



Implémenter le mixed mode



Mohamed Anass EDDIK

Une formation
Alphorm.com

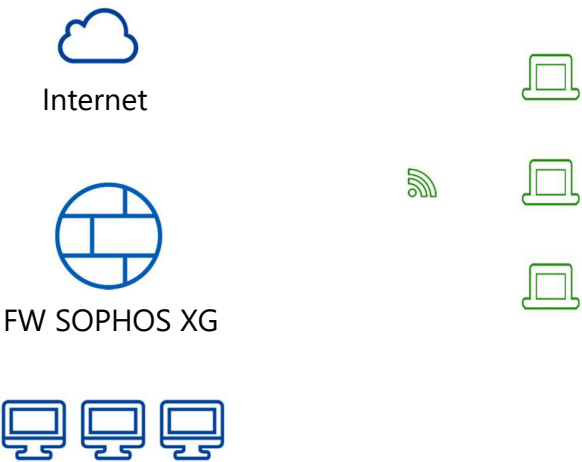


Plan

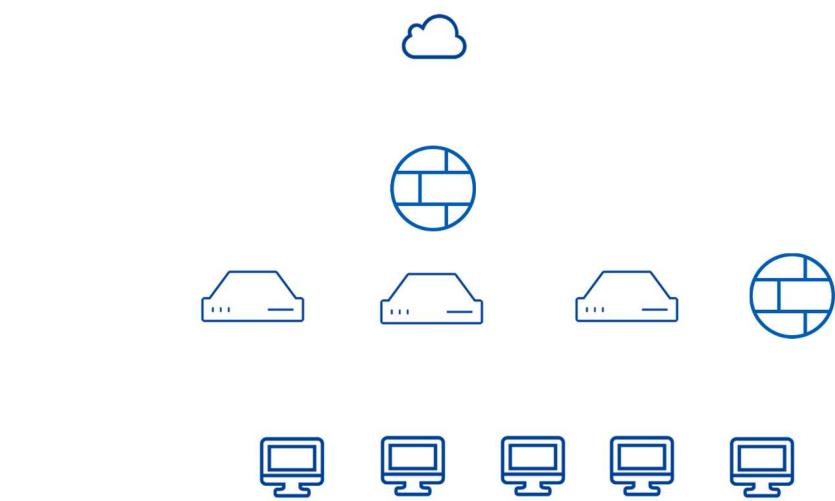
Scénario LAN
Scénario WAN

Une formation
Alphorm.com

Scénario WAN

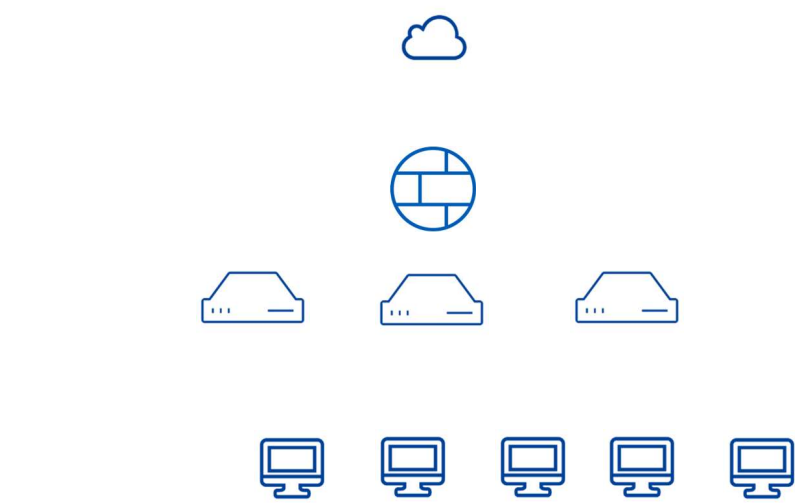


Scénario WAN



Une formation
Alphorm.com

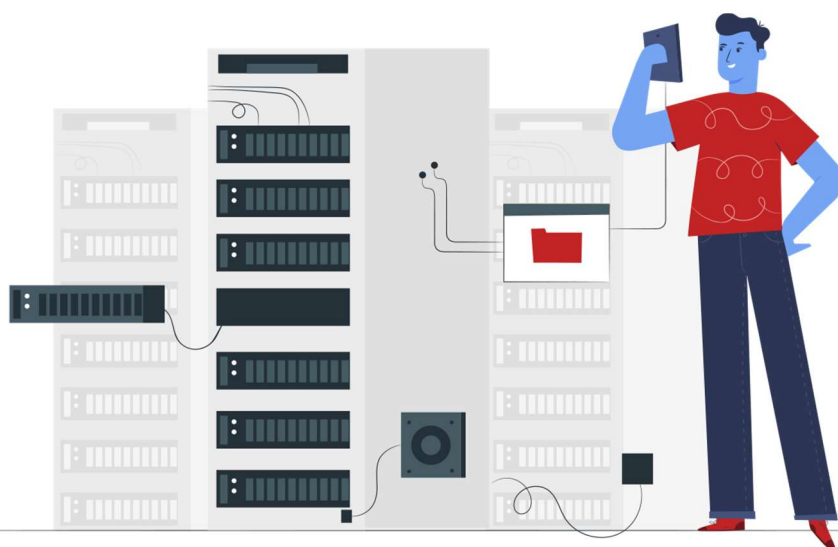
Scénario WAN



Une formation
Alphorm.com



Démo



Une formation
Alphorm.com



Implémenter le mixed mode *LAB*

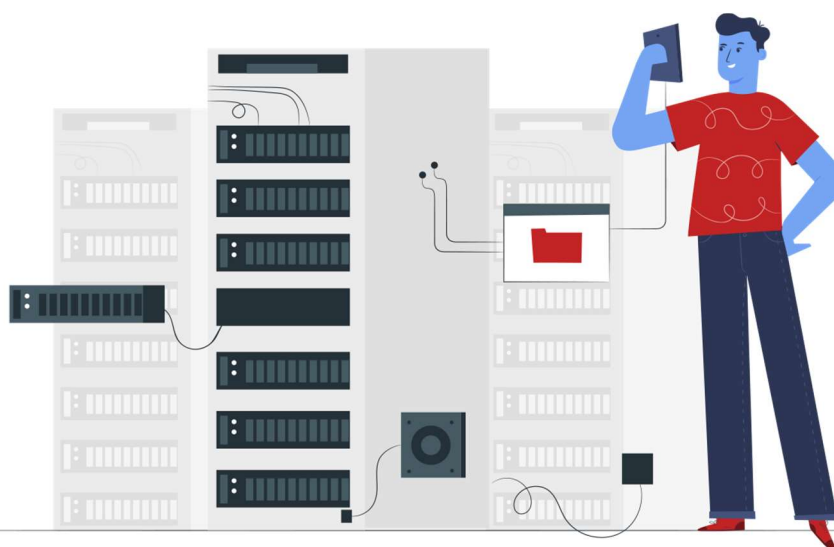


Mohamed Anass EDDIK

Une formation
Alphorm.com



Démo



Une formation
Alphorm.com



Gérer le Discover Mode



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

Discover Mode Firewall Framework

Une formation
Alphorm.com

Discover Mode



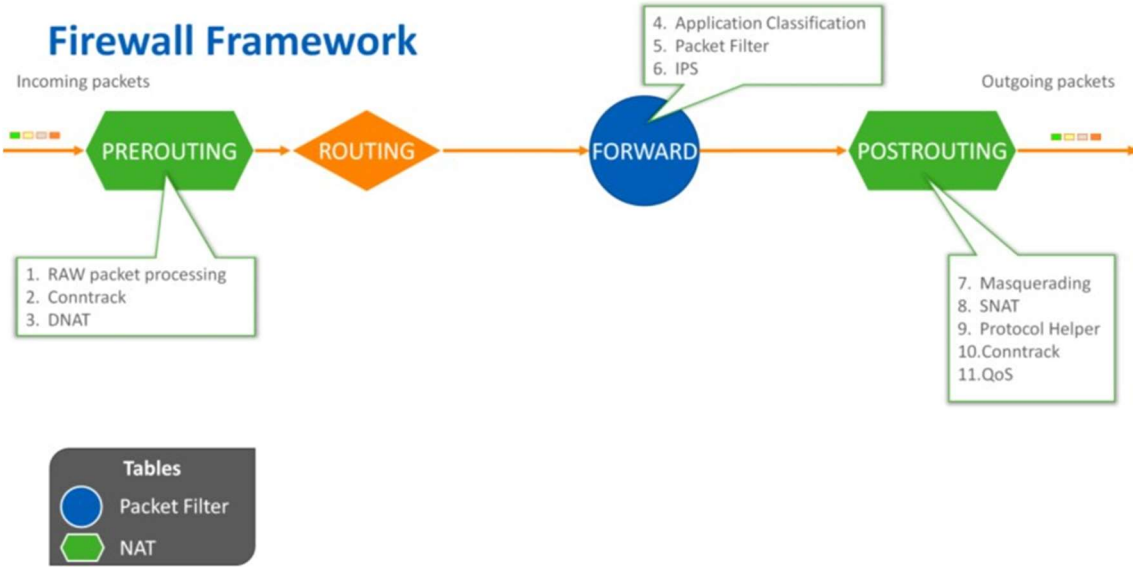
Internet



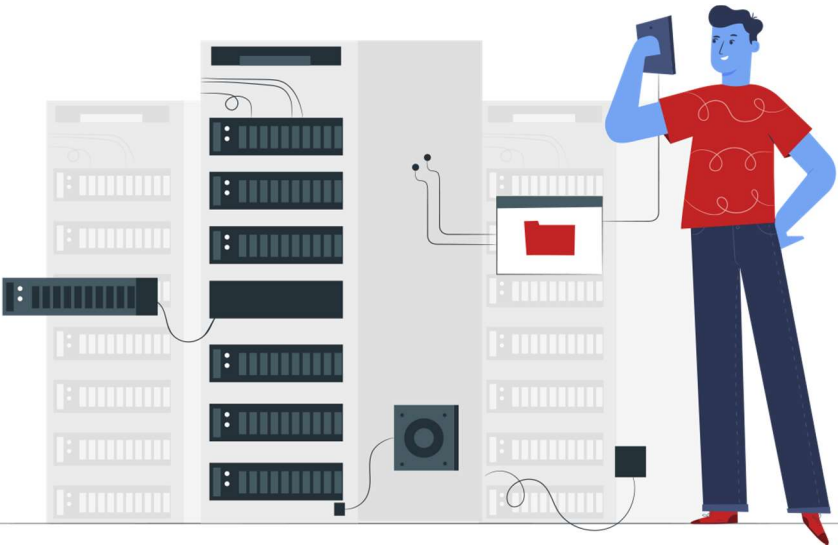
FW SOPHOS XG



Firewall Framework



Démo





Ajouter des interfaces et Routage avancé



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

Policy Routing
Routage Dynamique

Une formation
Alphorm.com



Policy Routing

Une formation
Alphorm.com



Routage Dynamique

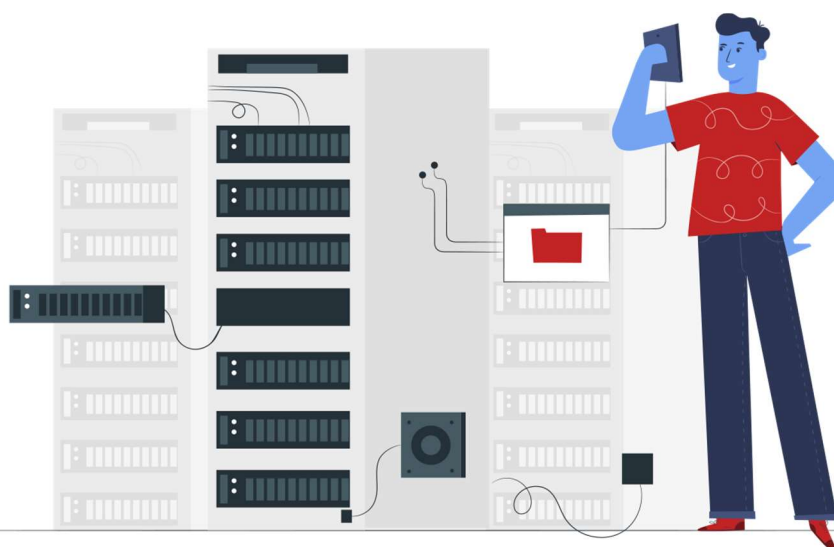
RIP

OSPF

Une formation
Alphorm.com



Démo



Une formation
Alphorm.com



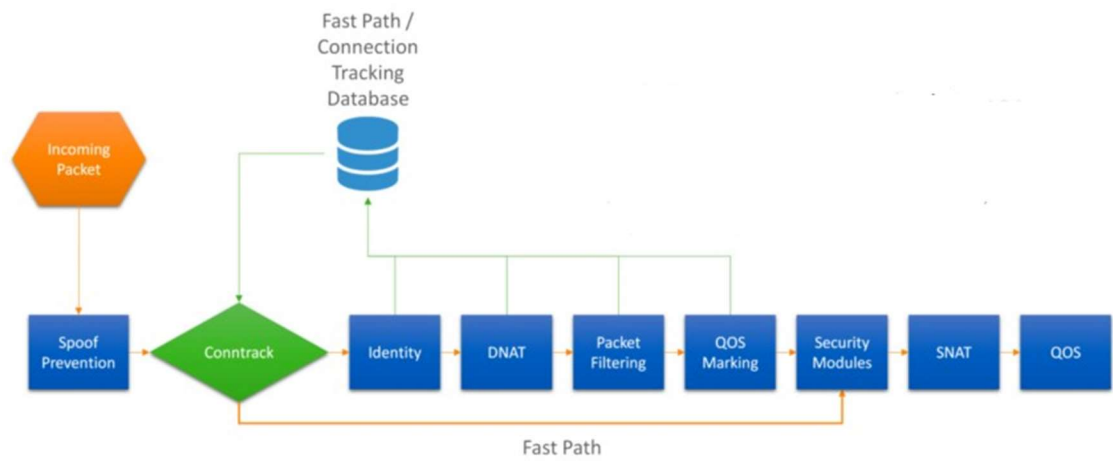
Comprendre la technologie "Fast Path"



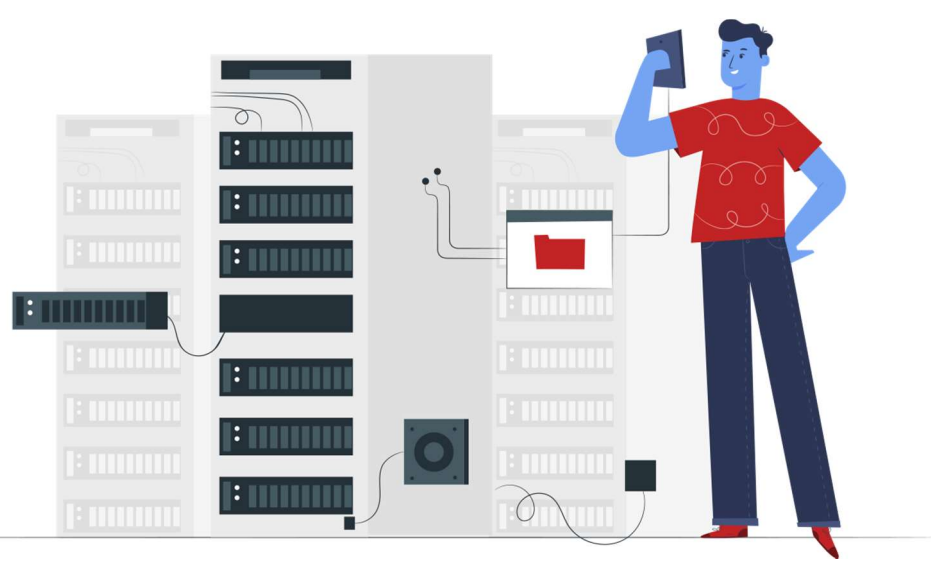
Mohamed Anass EDDIK

Une formation
Alphorm.com

Fast Path



Démo





Appliquer le Tunning sur l'IPS Policies



Mohamed Anass EDDIK

Une formation
Alphorm.com



Configurer l'IPS avancé



Mohamed Anass EDDIK

Une formation
Alphorm.com



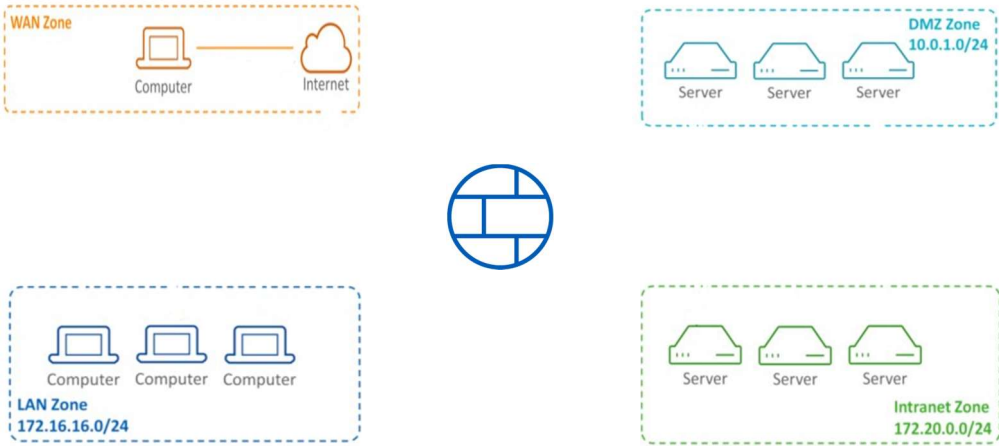
Protéger l'infra contre les attaques DOS



Mohamed Anass EDDIK

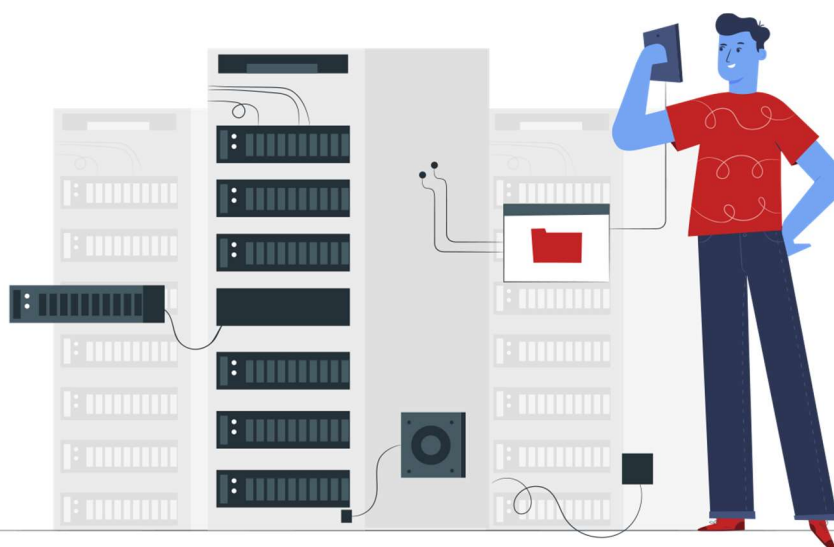
Une formation
Alphorm.com

Protection DoS avancée





Démo



Une formation
Alphorm.com



Gérer le NAT et le Traffic Shaping



Mohamed Anass EDDIK

Une formation
Alphorm.com



Appliquer les Fonctionnalités de protection



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

Cookie Signing
Web server Authentication

Une formation
Alphorm.com

Cookie Signing

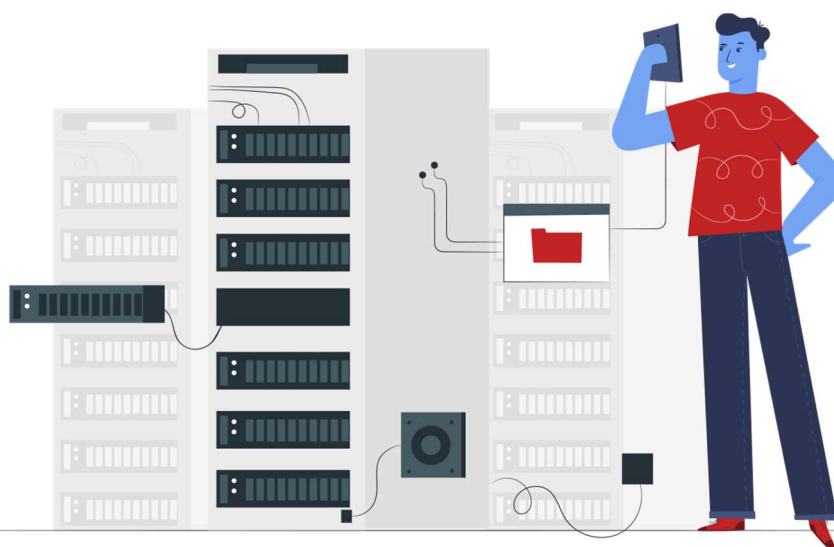


Web server Authentication





Démo



Une formation
Alphorm.com



Router un chemin spécifique



Mohamed Anass EDDIK

Une formation
Alphorm.com



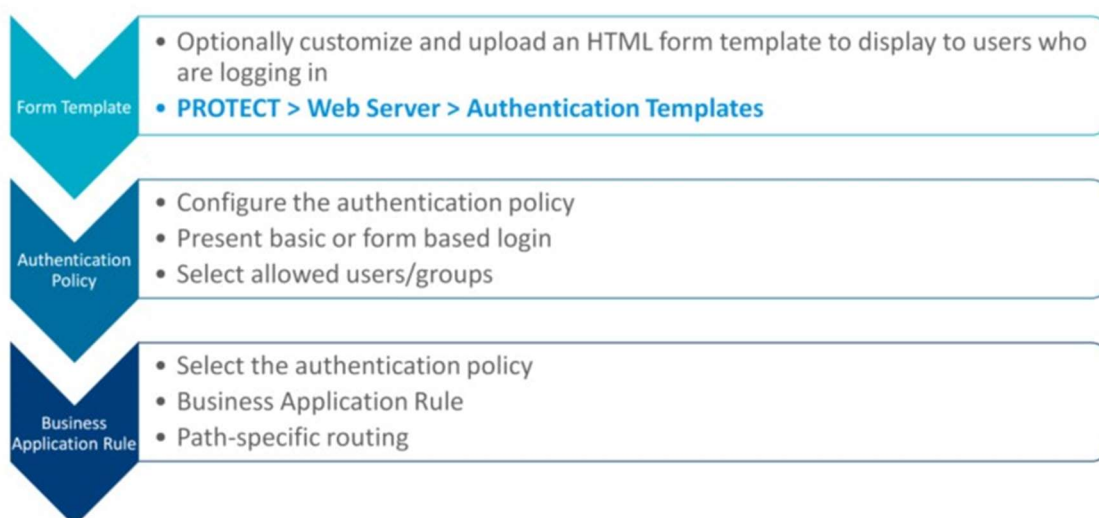
S'authentifier sur un Web Server



Mohamed Anass EDDIK

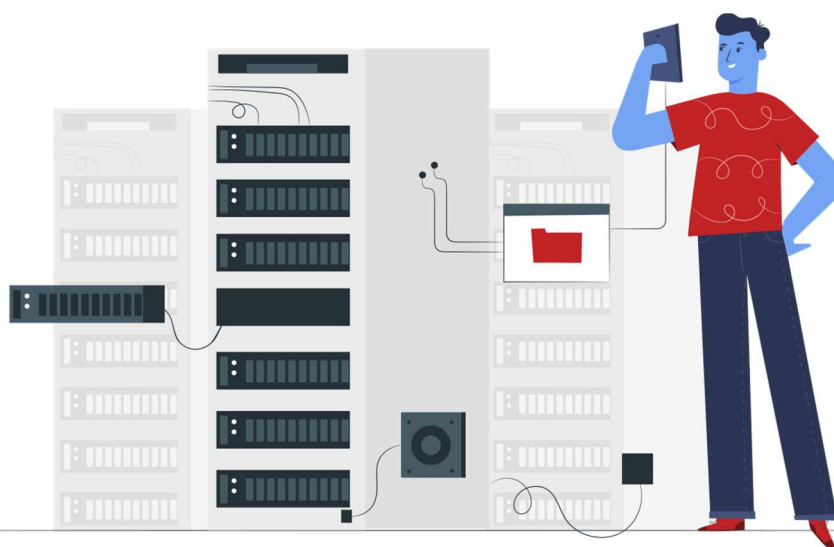
Une formation
Alphorm.com

Web Server Authentication





Démo



Une formation
Alphorm.com



Configurer le VPN site-to-site



Mohamed Anass EDDIK

Une formation
Alphorm.com



S'authentifier avec un certificat



Mohamed Anass EDDIK

Une formation
Alphorm.com

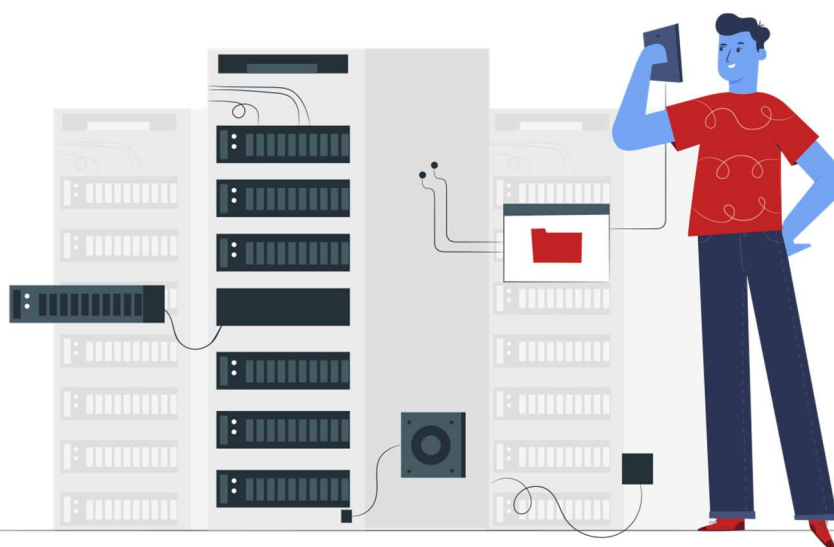


Certificate Authentication

Une formation
Alphorm.com



Démo



Une formation
Alphorm.com



Configurer le NAT Overlap



Mohamed Anass EDDIK

Une formation
Alphorm.com



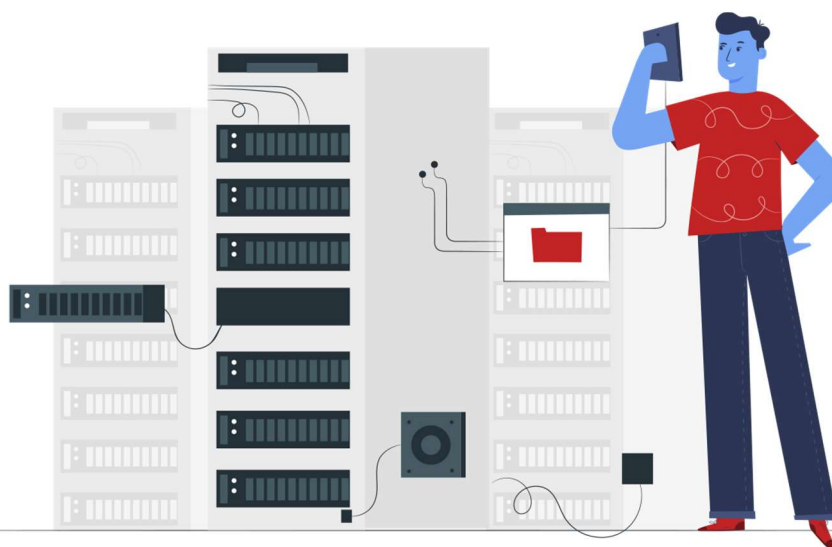
C'est quoi le NAT Overlap ?



Une formation
Alphorm.com



Démo



Une formation
Alphorm.com



Gérer le VPN Failover



Mohamed Anass EDDIK

Une formation
Alphorm.com

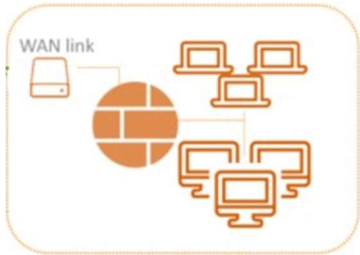
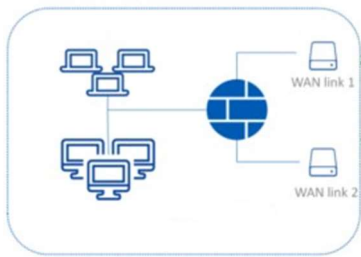


Plan

VPN Failover
VPN Failover link Multiple

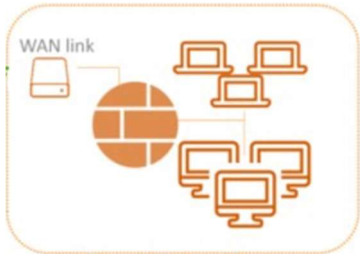
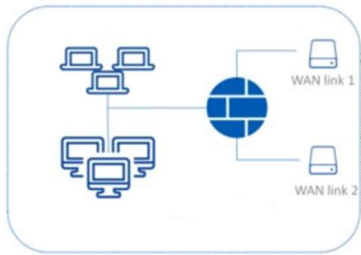
Une formation
Alphorm.com

VPN Failover



Une formation
Alphorm.com

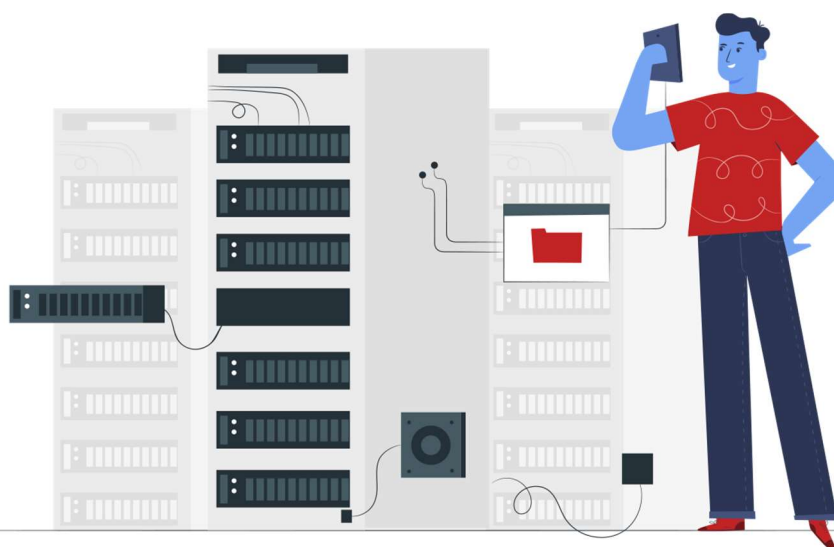
VPN Failover link multiple



Une formation
Alphorm.com



Démo



Une formation
Alphorm.com



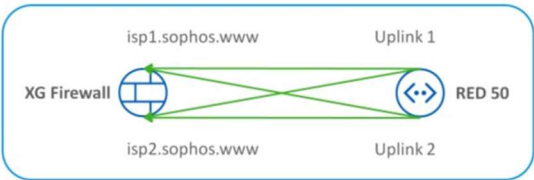
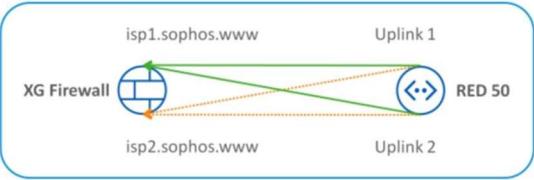
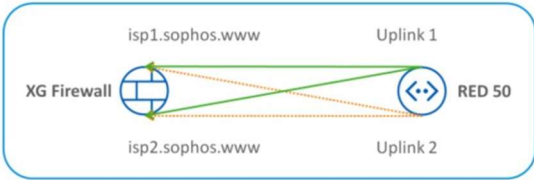
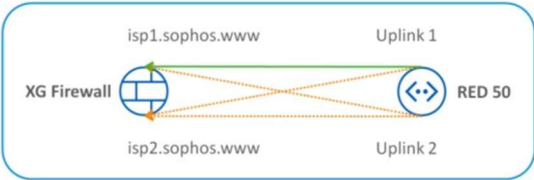
Manager les RED



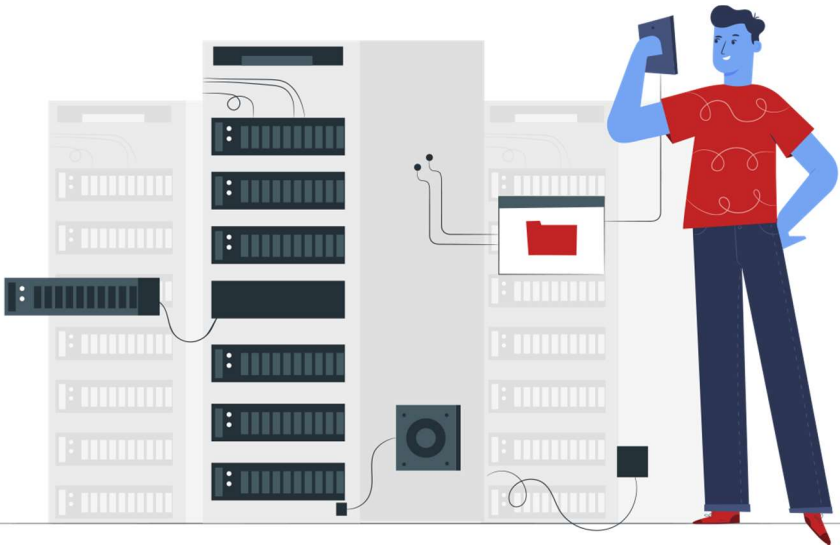
Mohamed Anass EDDIK

Une formation
Alphorm.com

Load balancing and Failover



Démo





Découvrir le Réseau Mesh

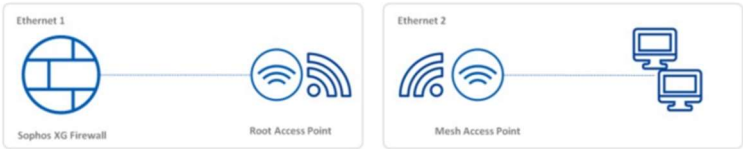


Mohamed Anass EDDIK

Une formation
Alphorm.com

Type de réseau Mesh

Wireless bridge

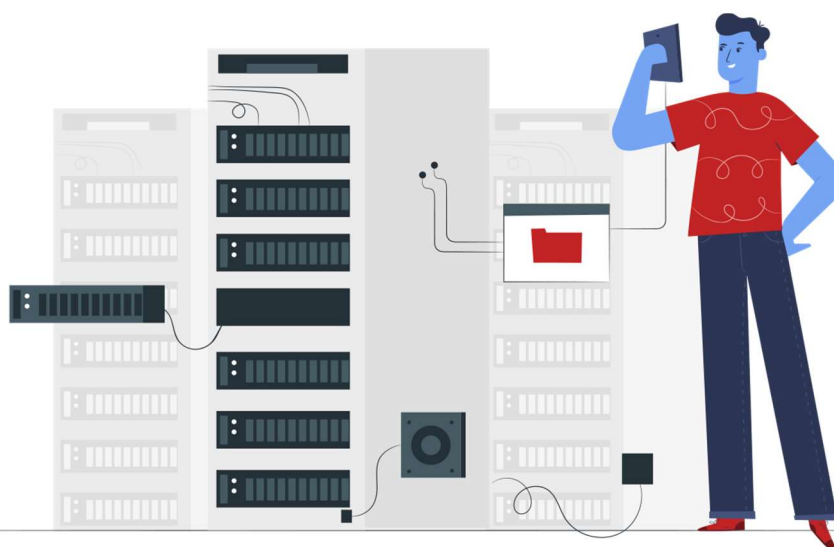


Wireless repeater





Démo



Une formation
Alphorm.com



Performance et déploiement



Mohamed Anass EDDIK

Une formation
Alphorm.com



Plan

Performance
Problème de déploiement

Une formation
Alphorm.com



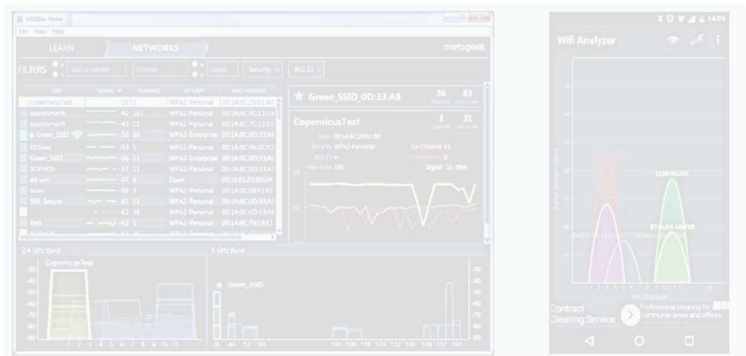
Performance

Une formation
Alphorm.com

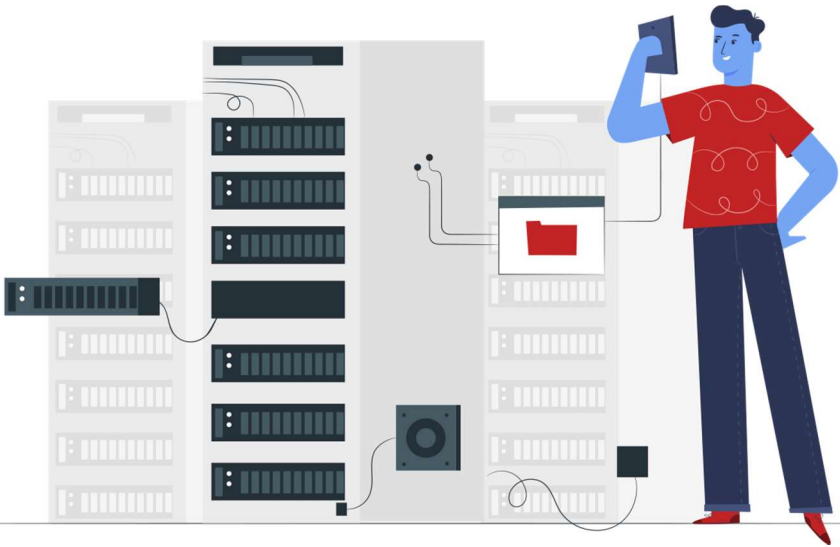


Problème de performance

Couverture
Interférence
Utilisation de fréquence



Démo





Comprendre le HA Packet flow

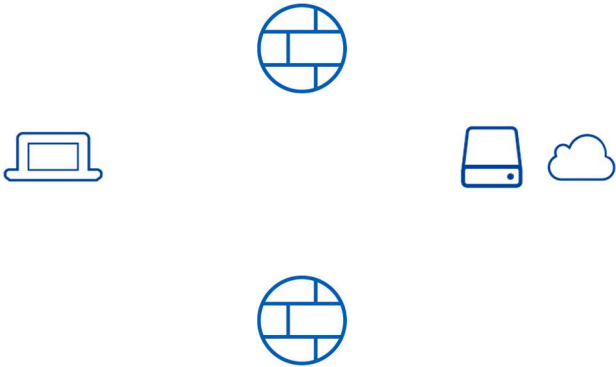


Mohamed Anass EDDIK

Une formation
Alphorm.com



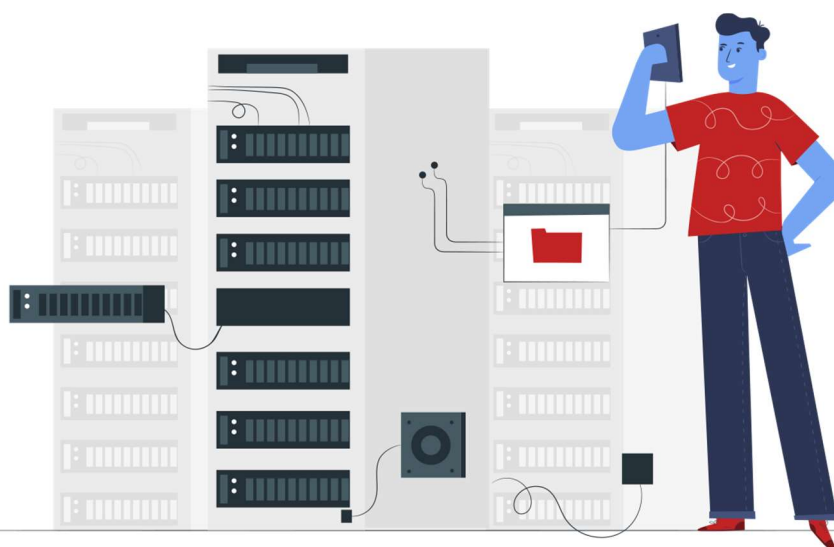
HA Packet Flow



Une formation
Alphorm.com



Démo



Une formation
Alphorm.com



Configurer le HA



Mohamed Anass EDDIK

Une formation
Alphorm.com



Utiliser le TCPDUMP



Mohamed Anass EDDIK

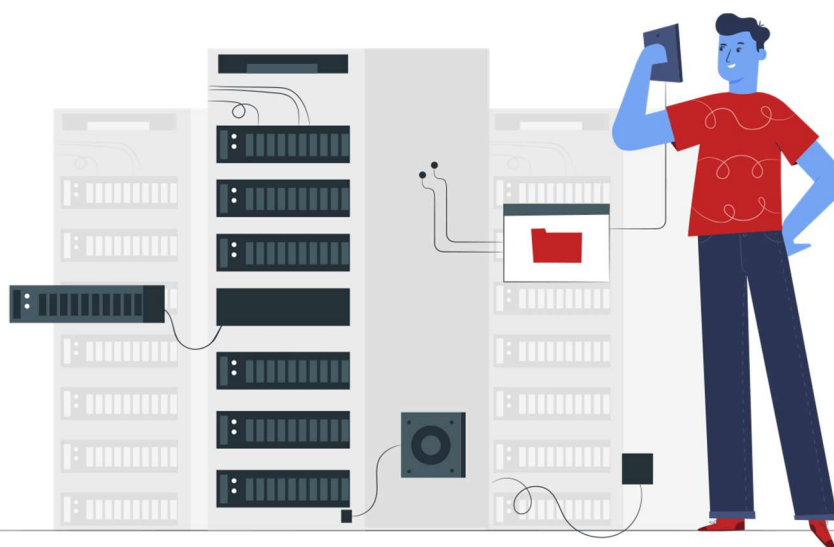
Une formation
Alphorm.com

TCPDUMP

How to view traffic of the...	tcpdump command	Example
specific host	tcpdump 'host <ipaddress>'	tcpdump 'host 10.10.10.1'
specific source host	tcpdump 'src host <ipaddress>'	tcpdump 'src host 10.10.10.1'
specific destination host	tcpdump 'dst host <ipaddress>'	tcpdump 'dst host 10.10.10.1'
specific network	tcpdump 'net <network address>'	tcpdump 'net 10.10.10'
specific source network	tcpdump 'src net <network address>'	tcpdump 'src net 10.10.10'
specific destination network	tcpdump 'dst net <network address>'	tcpdump 'dst net 10.10.10'
specific port	tcpdump 'port <port-number>'	tcpdump 'port 21'
specific source port	tcpdump 'src port <port-number>'	tcpdump 'src port 21'
specific destination port	tcpdump 'dst port <port-number>'	tcpdump 'dst port 21'
specific host for the particular port	tcpdump 'host <ipaddress> and port <port-number>'	tcpdump 'host 10.10.10.1 and port 21'
the specific host for all the ports except SSH	tcpdump 'host <ipaddress> and port not <port-number>'	tcpdump 'host 10.10.10.1 and port not 22'
specific protocol	tcpdump 'proto ICMP' tcpdump 'proto UDP' tcpdump 'proto TCP' tcpdump 'arp'	
particular interface	tcpdump interface <interface>	tcpdump interface PortB
specific port of a particular interface	tcpdump interface <interface> 'port <port-number>'	tcpdump interface PortB 'port 21'



Démo



Une formation
Alphorm.com



Consolider les rapports



Mohamed Anass EDDIK

Une formation
Alphorm.com



Gérer le Debug logging



Mohamed Anass EDDIK

Une formation
Alphorm.com



Conclusion



Mohamed Anass EDDIK

Une formation
Alphorm.com



Bilan

Déployer Sophos en entreprise
Configurer le Firewalling Avancé
Gérer Webserver protection
Configurer le VPN pour entreprise
Gérer le HA et le WIFI sur un XG
Dépanner sur XG FW

Une formation
Alphorm.com



Cursus Sophos XG 17.5



Sophos XG Certified Engineer

Sophos XG Certified Architect

Une formation
Alphorm.com

