Mise en œuvre de services sur le Pare Feu Stormshield

Yasmina Ramrani, Denis Wagner, Xavier Duthilleul

20 Juillet 2016

Plan de l’exposé

- Quels sont les besoins ?
- Quels sont les objectifs ?
- Pourquoi un IPS Stormshield ?
- Présentation du Stormshield
- Accès distant sécurisé : VPN SSL
- Le portail d’accès
- Le filtrage des URLs
- Démonstration
- HowTo disponibles
- Conclusion

Quels sont les besoins ?

- Mise en place d'un service d'accès à distance à certaines ressources internes du laboratoire
- Mise en place du filtrage d'URL et de blocage d'applications spécifiques
- Permettre l'accès aux ressources internes à partir de différents clients
- Authentification par un annuaire LDAP ou à défaut d'un annuaire interne
- Mise en place d'un portail d'accès aux ressources de type web

Quels sont les objectifs ?

7 laboratoires utilisent les IPS Stormshield?

- Mutualiser les connaissances

  -> Choix et mise en œuvre des services

  -> Ecrire et partager des procédures éprouvées, HowTo

  -> Communiquer sur des points particuliers

  -> Se rendre disponible ponctuellement ???

  -> Eclairer le choix d'autres laboratoires

  -> Référent ???

Pourquoi un IPS Stormshield ?

- Historique Netasq
- C’est un élément

  -> de sécurité

  -> de structuration du réseau

  -> **fournisseur de services**, …
- Expertise distributeur, SAV, maintenance
- « Relative » facilité de configuration
- Suivi & évolution
- Approche globale de la sécurité: réseau, données, postes, …

~~-> !!?? Oui mais cela coûte cher !!??~~

Présentation du Stormshield

Spécifications des solutions matérielles

	Petites entreprises, Agences, Filiales			Moyennes organisations, Agences			Grandes organisations, Datacenters		
	SN150	SN200	SN300	SN510	SN710	SN910	SN2000	SN3000	SN6000
PERFORMANCES*									
Débit Firewall (UDP 1518 octets)	400 Mbps	600 Mbps	800 Mbps	5 Gbps	10 Gbps	20 Gbps	30 Gbps	50 Gbps	130 Gbps
Débit IPS (UDP 1518 octets)	200 Mbps	600 Mbps	800 Mbps	3 Gbps	7 Gbps	12,5 Gbps	20 Gbps	30 Gbps	55 Gbps
Débit IPS (1 Mo HTTP)	150 Mbps	600 Mbps	800 Mbps	1,7 Gbps	2,6 Gbps	7 Gbps	12 Gbps	14 Gbps	17 Gbps
Débit Antivirus	55 Mbps	165 Mbps	200 Mbps	850 Mbps	1,6 Gbps	2,2 Gbps	3,2 Gbps	4 Gbps	4,7 Gbps
CONNECTIVITÉ RÉSEAU									
Nb max. de sessions simultanées	30 000	75 000	150 000	500 000	1 000 000	1 500 000	2 000 000	2 500 000	10 000 000
Nb de nouvelles sessions par sec.	2 500	15 000	18 000	20 000	40 000	60 000	90 000	120 000	180 000
VPN*									
Débit IPSec (AES128 – SHA1)	100 Mbps	250 Mbps	400 Mbps	1 Gbps	2,4 Gbps	4 Gbps	5 Gbps	6,5 Gbps	12 Gbps
Nb max. de tunnels VPN IPSec	25	50	100	500	1 000	1 000	5 000	5 000	10 000
Nb de clients VPN SSL simultanés	5	20	20	100	150	150	200	500	500
HAUTE DISPONIBILITÉ									
Actif/Passif	-	-	✓	✓	✓	✓	✓	✓	✓
CONNECTIVITÉ									
Interfaces 10/100/1000	1 + 4 ports (switch)	1 + 2x2 ports	8	12	8-16	8-16	10-26	10-26	10-58
Interfaces fibre 1Gb	-	-	-	-	0-4	0-6	0-16	0-16	0-56
Interfaces fibre 10Gb	-	-	-	-	0-2	0-2	0-8	0-8	0-28
HARDWARE									
Redondance (SSD, Alimentation)	-	-	-	-	-	-	-	✓	✓
Stockage local	-	SD Card**	SD Card**	320 GB	320 GB	128 GB SSD	128 GB SSD	128 GB SSD	256 GB SSD
Taille	<0,5U - 19"	0,5U - 19"	0,5U - 19"	1U - 19"	1U - 19"	1U - 19"	1U - 19"	1U - 19"	2U - 19"

Présentation du Stormshield

De base : mise à jour automatique

- Anti-Spam basé sur des listes noires
- Moteur de prévention d'intrusion IPS (bases ciblées)
- Antivirus Clamav
- Base d'URLs embarquée
- Autorité de certification

En option :

- Détection en temps réel d'applications obsolètes, de vulnérabilités sur les postes/serveurs

Présentation du Stormshield

Les +

- Maintenance
- Blocage d’applications (exp.: Teamviewer, …)

Les -

- Documentation générale mais pas de procédure

Accès distant sécurisé: VPN SSL

Objectifs

- De l'Internet, permettre l'accès distant à une machine, aux partages, aux imprimantes, … du réseau interne

Comment

- Créer un réseau dédié qui sera assigné aux utilisateurs du VPN
- Activer et configurer le module VPN SSL
- Activer le portail VPN SSL pour indiquer l'accès aux serveurs applicatifs/web
- Définir le type d'authentification des utilisateurs
  - -> annuaire LDAP existant
  - -> annuaire LDAP interne au pare-feu
  - -> radius/kerberos (non testé)
- Activer l'autorisation des utilisateurs à utiliser le VPN SSL

Accès distant sécurisé: VPN SSL

- Définir les règles de filtrage aux ressources/utilisateur
- Installer un certificat DigiCert pour le portail captif et le VPN SSL

Possibilités:

- Mettre en place une translation d’adresse pour des besoins spécifiques

Accès distant sécurisé: VPN SSL

Installation des clients

- Windows : Le client VPN SSL est téléchargeable sur le portail d'accès du pare-feu
- Linux : le profil est téléchargeable sur le portail d'accès du pare-feu, un client openvpn dans les dépôts
- Mac OSX : le profil est téléchargeable sur le portail d'accès du pare-feu, un client openvpn : https://tunnelblick.net/
- Android , IOS : le profil est téléchargeable sur le portail d'accès du pare-feu, un client Open VPN Connect dans le Store

Accès distant sécurisé: VPN SSL

Connexion des clients : Principe

- Connexion au serveur d'authentification du pare-feu
- Vérification des informations
- Contrôle dans les règles du droit à établir un tunnel
- Récupération de manière transparente sa configuration (profil de connexion , certificat, autorité de certification) pour la négociation du tunnel
- Enregistrement de l'utilisateur dans la tables des utilisateurs de l'ASQ
- Le client récupère une adresse IP et toutes les routes pour joindre les ressources internes
- Les accès sont gérés par la politique de sécurité et de filtrage

Le portail d’accès

Objectifs

De l’Internet, permettre l’accès aux serveurs Web et applicatifs du réseau interne par le portail captif.

Connexion des clients : Principe

- Connexion au serveur d’authentification du pare-feu
- Vérification des informations
- Récupération de manière transparente sa configuration (sites web & applications)
- Enregistrement de l’utilisateur dans la tables des utilisateurs de l’ASQ
- Les accès sont gérés par la politique de sécurité et de filtrage

Le filtrage des URLs

Objectif

- Blocage d'un site/ plusieurs sites

Comment

- Le site est existe dans une catégorie de filtrage embarqué alors changer l'action par bloquer (par défaut = passer)
- Laisser la page de blocage par défaut ou créer une page de blocage personnalisée
- Mettre en place un filtrage personnalisé :
  -> ajouter une catégorie
  -> insérer le ou les sites à bloquer
  -> activer le filtrage et indiquer la page de blocage
- Vérifier !!!
- Attention: pour https, il faut créer une règle de déchiffrement qui génère une alerte dans le navigateur

HowTo disponibles

HowTo (White paper) disponibles assez restreints… et parce que les approches sont souvent similaires dans nos labos…

- Maintenance

-> Mise à jour de la version du logiciel de l'IPS Stormshield

- Filtrage

-> Filtrage d'un URL ou d'une liste d'URLs

- Configuration du VPN SSL

-> Installation Certificat Digicert Stormshield

-> Configuration du VPN SSL sur Stormshield

-> Installation du client VPN sous Android

HowTo disponibles

-> Installation du client VPN sous IPAD
-> Installation du client VPN sous LINUX
-> Connexion au VPN depuis LINUX
-> Installation du client VPN sous Macintosh
-> Connexion au VPN depuis Macintosh
-> Installation du client VPN sous Windows
-> Connexion au VPN depuis Windows

https://tapas.unistra.fr/securite/stormshield

D’autres HowTo ?

Sans se substituer aux interlocuteurs « Stormshield »,

si vous avez une expertise dans un domaine spécifique,

Partagez là SVP !

-> Vlans,
-> NAT,
-> DHCP,
-> Services optionnels , …

Conclusion

- Mutualiser les connaissances
- Participez à la mutualisation de vos connaissances
- Soutien aux labos en phase de réflexion concernant le choix d'un IPS

Démonstrations

- Accès à distance aux PC du laboratoire:
    1) Connexion au VPN,
    2) Démarrage du PC,
    3) Bureau à distance

- Accès aux services internes du laboratoire:
    1) Comptes de l’Active Directory,
    2) Portail d’accès.

Merci de votre attention

/

QUESTIONS