



Guide d'utilisation du service CyberVigilance

TABLE DES MATIERES

Information	3
Authentification	4
Accès à l'interface CyberVigilance	5
Navigation sur l'interface	6
Accès au rapport.....	6
Accès plateforme avancée CyberVigilance	11

INFORMATION

Ce service a pour but de renforcer la sécurité du réseau de votre étude.

L'interface qui vous sera présentée ci-après va vous permettre de consulter les rapports de sécurité de votre routeur navista.

En cas de difficultés, vous pouvez joindre le support navista :

Service support navista :



04 68 68 69 77



support@navista.fr

Horaire d'ouverture du service support :

Du lundi au vendredi : 8h30 à 21h

Le samedi : 8h30 à 12h

AUTHENTIFICATION

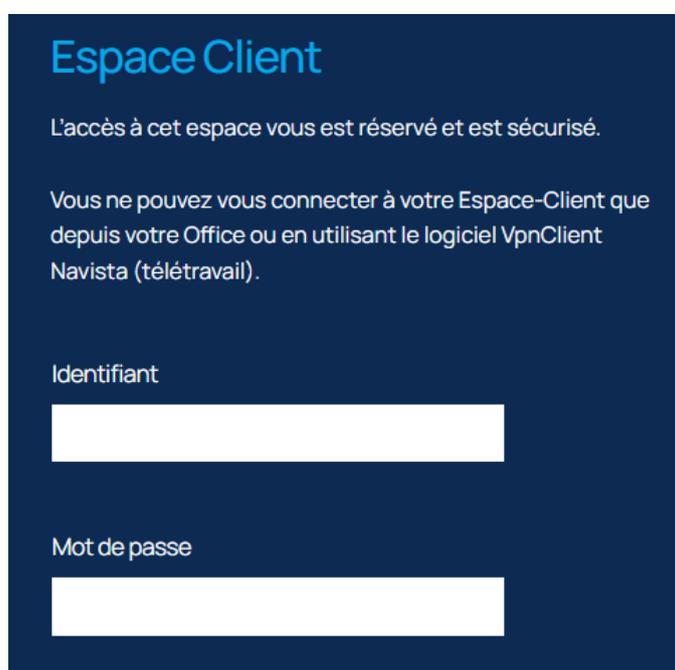
Afin de vous connecter aux services de CyberVigilance, se rendre sur le site

<https://www.navista.fr>

Cliquer sur : « Connexion à l'Espace client » dans le bandeau de présentation du site



Saisissez vos informations de connexion puis cliquer sur « Se connecter »

The screenshot shows a dark blue login page titled 'Espace Client'. Below the title, there is a message: 'L'accès à cet espace vous est réservé et est sécurisé.' followed by 'Vous ne pouvez vous connecter à votre Espace-Client que depuis votre Office ou en utilisant le logiciel VpnClient Navista (télétravail)'. There are two input fields: 'Identifiant' and 'Mot de passe', both with white text boxes. The 'Mot de passe' field has a small eye icon to its right.

Rentrer le code de sécurité reçu par SMS ou sur votre application de double authentification et cliquer sur « Envoyer »

The screenshot shows a 'Connexion' form. At the top, there is a green notification box with a close icon (X) and the text: 'Un SMS contenant un code de sécurité unique vous a été envoyé. Merci de saisir ce code dans la fenêtre ci-dessous.' Below this is a light blue input field with a lock icon and the text 'Code de sécurité'. At the bottom of the form is a dark blue button labeled 'Envoyer'. Below the button is a link that says 'Demander un nouveau code'.

ACCES A L'INTERFACE CYBERVIGILANCE

Cliquer sur la « Rapport Réseau / CyberVigilance »



Par défaut, vous êtes sur la page d'accueil CyberVigilance

Liste des Offices et annexes

CRPCEN	Site	VpnRouter	Rapport Réseau / CyberVigilance	Abonnement CyberVigilance
99053	Navista Support Test	✓

Network Manager
Pour valider votre accès au portail monitoring de votre VpnRouter, merci de vous rapprocher du service support navista (accessible au 04 68 68 69 77 et sur support@navista.fr) qui vous accompagnera dans la création de votre accès privilégié.

Vous retrouvez le portail auquel vous accédez pour :

- Gérer les VPN Télétravail
- Envoyer des fichiers volumineux
- Consulter l'état et les dernières informations concernant votre éligibilité
- Visualiser les services et les rapports CyberVigilance
- Accéder aux services de VisioConférence
- Accéder à vos factures

NAVIGATION SUR L'INTERFACE

ACCES AU RAPPORT

Pour accéder aux rapports disponibles par site ainsi qu'à la liste des services activés ou non sur votre VpnRouter de raccordement, il vous suffit à présent de cliquer sur le symbole .



Services CyberVigilance

Service	Activé	Description
IDS/IPS	<input checked="" type="checkbox"/>	L'IDS (Intrusion Detection System) est le composant sécurité de la CyberVigilance qui détecte les activités anormales ou suspectes sur le Réseau local de votre Office. Il permet ainsi d'alerter sur les tentatives d'intrusion sur votre Réseau local. Il existe deux grandes catégories d'IDS; les plus connues sont les détections par signatures (reconnaissance de programme malveillant) et les détections par anomalies (détecter les écarts par rapport à un modèle représentant les bons comportements, par de l'apprentissage automatique, aussi appelé machine learning). L'IPS (Intrusion Prevention System) est le composant sécurité de la CyberVigilance, complémentaire à l'IDS, qui bloque les flux intrusifs provenant d'Internet au sein du Réseau local de votre Office.
Anti Malware	<input checked="" type="checkbox"/>	L'Anti Malware est le module sécurité de la CyberVigilance qui bloque l'accès aux sites considérés comme malveillants. La liste des sites pour l'Anti Malware est mise à jour quotidiennement.
Firewall (Pare Feu)	<input checked="" type="checkbox"/>	Le Firewall (Pare feu) régule le trafic vers votre Office selon les règles de sécurité pré-établies. Il n'accepte que les flux autorisés et rejette toute tentative d'accès non autorisés.
Filtrage WEB	<input checked="" type="checkbox"/>	Le Filtrage WEB filtre (autorise ou bloque) l'accès aux sites internet selon leur catégorisation. Il empêche ainsi l'accès à tout site au contenu malveillant (terrorisme, racisme) ou non souhaité (pornographie).
Filtrage applicatif	<input checked="" type="checkbox"/>	Le Filtrage applicatif réalise le filtrage des communications suivant les différents protocoles comme Spotify, Deezer, téléchargement de films, jeux en lignes, télé ou radio en ligne. Le Filtrage applicatif bloque ou autorise les flux selon les règles pré-établies.
QoS applicative	<input checked="" type="checkbox"/>	La QoS applicative permet la priorisation des flux en fonction de leur nature (application temps réel, téléphonie IP, VisioConférence) et de leur criticité (flux métiers, CDC, MICEN, cadastre...)

IMPORTANT : les rapports sont générés tous les lundis matin et contiennent les données relevées la semaine précédentes.

Ci-dessous la liste des menus disponibles dans votre rapport

- État de fonctionnement
- Informations
- Disponibilité internet
- Bande passante
- Utilisation des ressources
- Performances des accès
- Disponibilités des VPN
- VpnClient (Télétravail)
- Filtrage WEB
- Qualité de service applicative
- IDS/IPS (Système de détection d'intrusion/Système de prévention d'intrusion)
- Anti-malware
- Firewall (Pare Feu)
- Trafics non autorisés

Nous vous présentons ci-dessous un résumé des menus contenus dans votre rapport.

Notre service support est à votre disposition afin de vous accompagner dans la compréhension globale de ce rapport.



Pour chaque menu, un texte explique le contenu de la section consultée

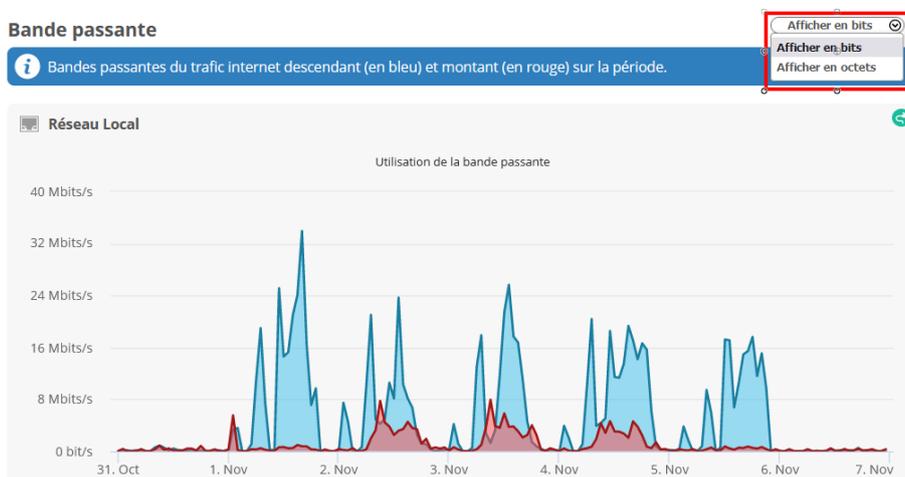
Disponibilité internet

Afficher en bits

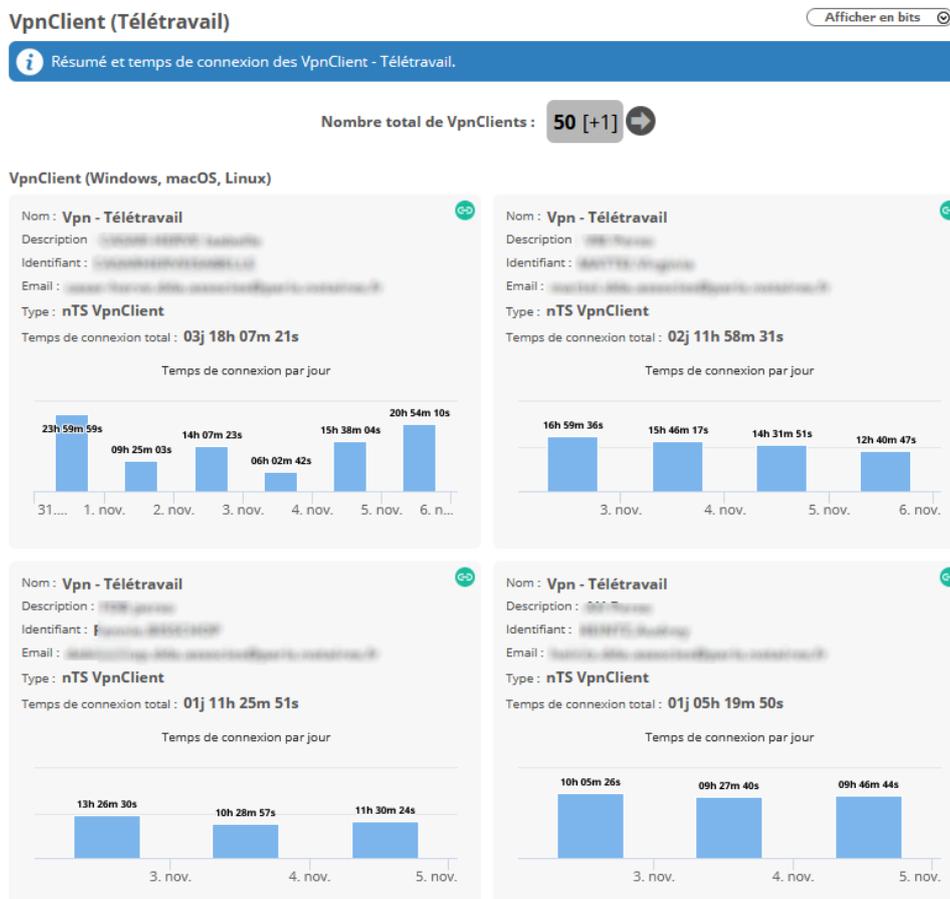
Indique le niveau de disponibilité des lignes internet raccordées sur le VpnRouter sur la période.
Les informations indiquées telles que le type de connexion, l'opérateur internet, etc.. sont issues de données communiquées par notre service technique ou par vos soins. Ces valeurs peuvent différer des valeurs réelles.

Type de liaison	Opérateur internet	Disponibilité
ADSL	orange	100% (+0.11%)
FIBRE	orange	100% (0%)
SDSL	OVH	99.98% (0%)

Selon le menu consulté, il est possible de sélectionner le type d'affichage désiré, en bits ou en octets

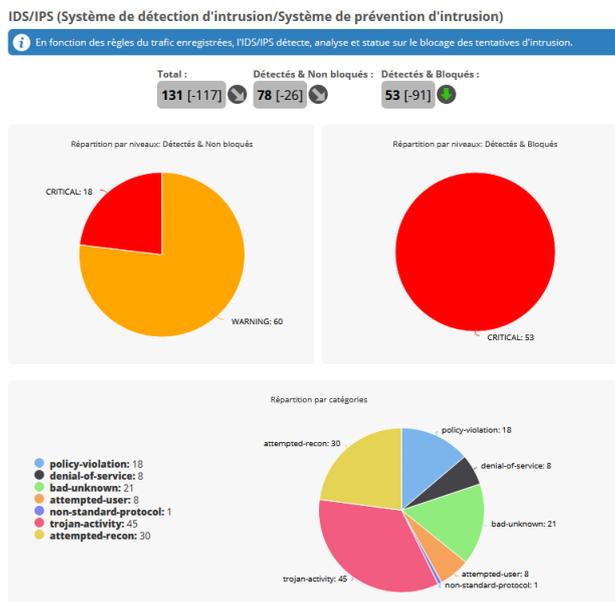


Vous pouvez consulter le temps de connexion des VPN, notamment les comptes télétravail

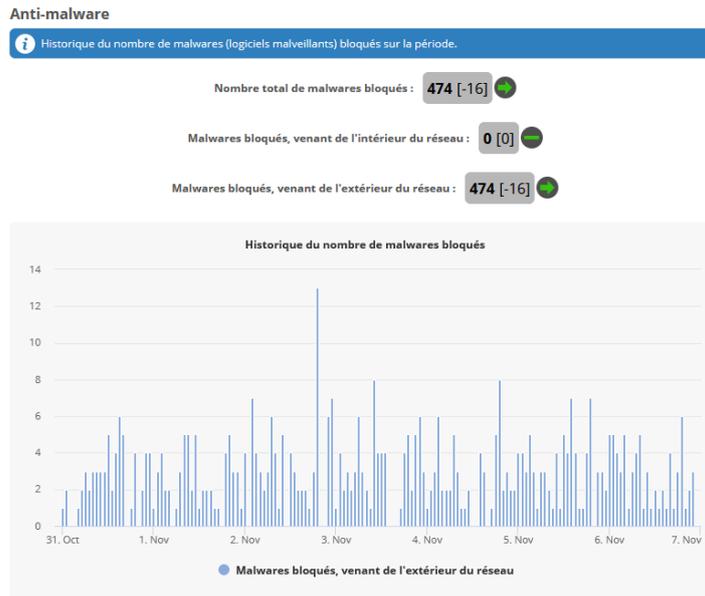


Dans la section spécifique à la CyberVigilance, vous trouverez plusieurs menus dont le celui de la détection et de prévention d'intrusion.

Ce menu illustrera les tentatives d'intrusions bloquées par le système



Le menu Anti-malware illustrera le nombre de logiciels malveillants bloqués par le système.



Nous vous rappelons que ce guide présente un résumé du rapport du service de CyberVigilance

Notre service support est à votre disposition afin de vous accompagner dans la compréhension globale de ce rapport.

ACCES PLATEFORME AVANCEE CYBERVIGILANCE

Il vous est possible d'accéder à une plateforme avancée du service de CyberVigilance. Cette plateforme s'adresse avant tout à un public ayant des connaissances approfondies en informatique et particulièrement au réseau informatique.

Vous pouvez accéder à cette plateforme de CyberVigilance sur simple demande à notre service Support.

Un guide détaillé d'utilisation de cette plateforme vous sera alors transmis.

IMPORTANT : Il vous est possible de déléguer l'accès à la plateforme de CyberVigilance à votre prestataire informatique afin qu'il dispose d'un outil performant de supervision, sans surcout.

Network Manager

Pour valider votre accès au portail monitoring de votre VpnRouter, merci de vous rapprocher du service support navista (accessible au 04 68 68 69 77 et sur support@navista.fr) qui vous accompagnera dans la création de votre accès privilégié.