How To Guide

The CTAP Process

FORTINET

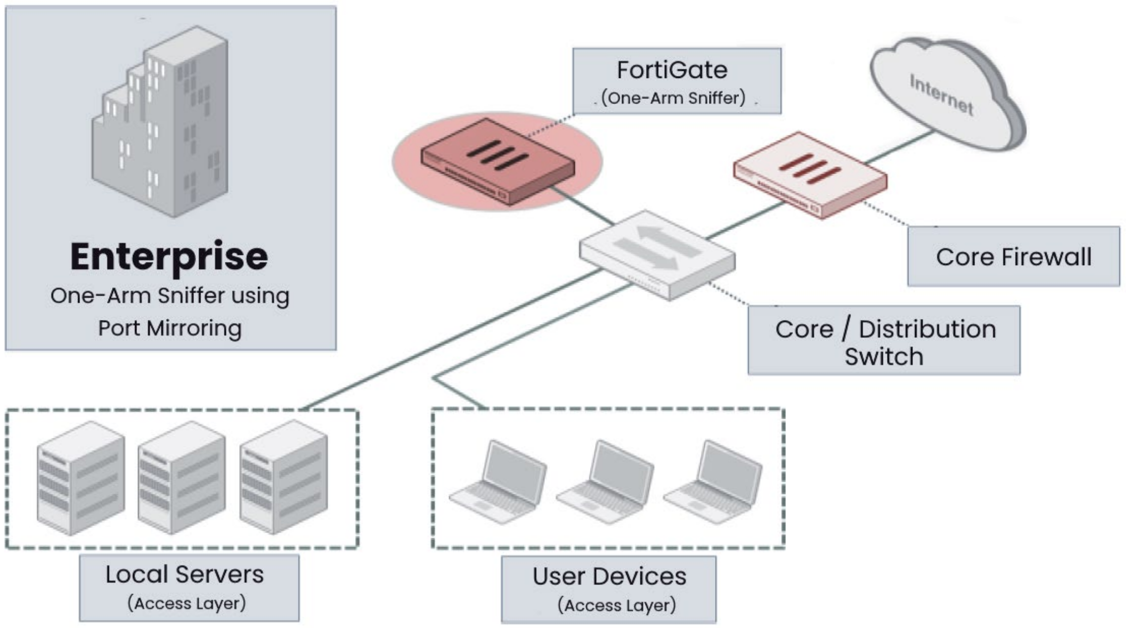
EXCLUSIVE NETWORKS

CTAP

A CTAP (Cyber Threat Assessment Program) involves the placement of a FortiGate unit behind a customer's existing Firewall to run an assessment of the effectiveness of their current security architecture.

The unit is left in place for 5-7 days to enable the monitoring of the network with metadata collected on the traffic and a detailed report generated highlighting network security effectiveness, vulnerabilities and threats, applications and web resources usage and network performance.

One-Arm Sniffer using Port Mirroring



Basic CTAP Process

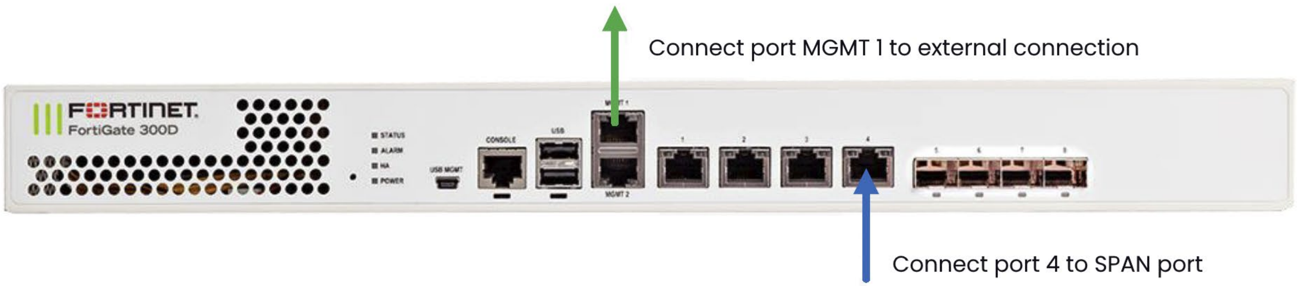
- Agree with customer to run a CTAP
  - Aim of CTAP
  - Proposed actions from the outcome of the activity
- Ensure appropriate ports, connectivity is available to run CTAP.
- Request a CTAP loan unit from Exclusive Networks
  - Complete loan form
  - Electronic sign off and approval
  - Unit shipped to end user/customer
- CTAP portal configured to enable CTAP unit to do reporting (requires unit serial number, customer details)
- Install CTAP unit on customer site and check unit is logging correctly.
- Leave unit running for approximately 7 days
- Generate report – triggered based on dates entered in CTAP Portal.
- Remove CTAP unit from site and return back to Exclusive Networks, onus on Partner to arrange and return unit in original packaging along with all cables, networks and power cords.
- Present report back to end user highlighting key areas and agree next steps.

For a complete tutorial on the Fortinet CTAP process, configuring portal, presenting the report back to customers please visit the HELP section on the Cyber Threat Assessment Portal. **https://ctap.fortinet.com**

CTAP Requirements

There are few things that are needed to be done prior to installation, do you have the following information and can the following conditions be met prior to the install.

- Provide an IP for the network: IP address and subnet mask required.
- Provide a default route which will provide access to the internet.
- Provide a DNS server address.
- A SPAN/Mirror port required and set up ready for connection with relevant network segments.
- Plug to power the unit



Connect port MGMT 1 to external connection

Connect port 4 to SPAN port

For a successful CTAP assessment, FortiGate employs several services from FortiGuard (service.fortiguard.net, www.fortiguard.com) for AV, IPS, Application Signatures as well as URL Categorization Services.

These must be allowed on the external firewall from the unit address to the internet.
Ports are listed as such:

- 53 and 8888 UDP – FortiGuard URL Categorization Services
- 123 TCP/UDP NTP – Time Sync
- 443 TCP HTTPS – FortiGuard AV, IPS Signatures
- 514 TCP/UDP RSH – Remote logging server

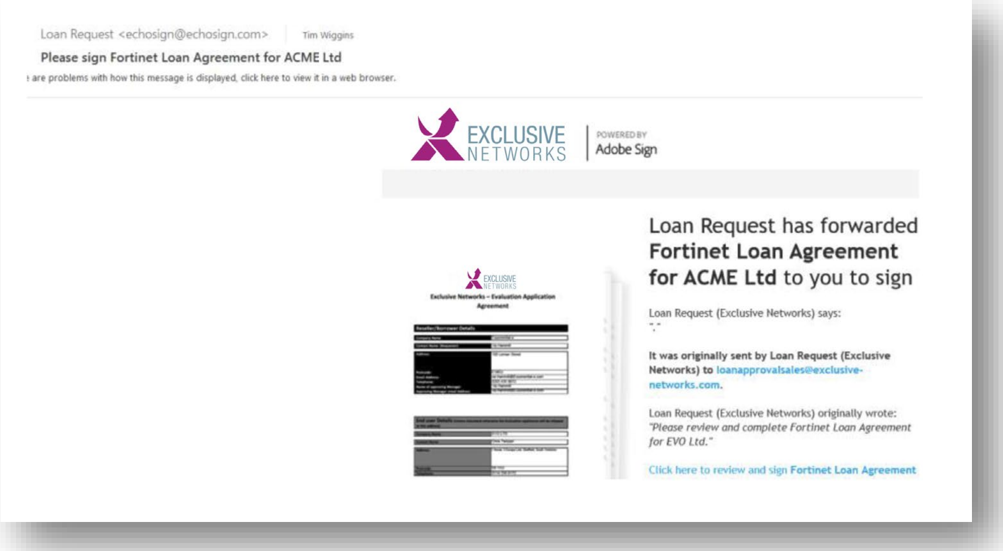
Request loan unit from Exclusive Networks

To request a loan unit an Exclusive Networks Evaluation Loan agreement needs to be complete and returned to your account manager.

This form starts the process for electronic signoff of the loan, ie the approving manager email address will receive an email from echosign@echosign.com to sign and approve the loan.

Loan Request echosign@echosign.com

The unit is then pre-staged and loaded with appropriate firmware and checked before being shipped.



Loan Request <echosign@echosign.com> | Tim Wiggins

Please sign Fortinet Loan Agreement for ACME Ltd

: are problems with how this message is displayed, click here to view it in a web browser.

Loan Request has forwarded **Fortinet Loan Agreement for ACME Ltd** to you to sign

Loan Request (Exclusive Networks) says:
" "

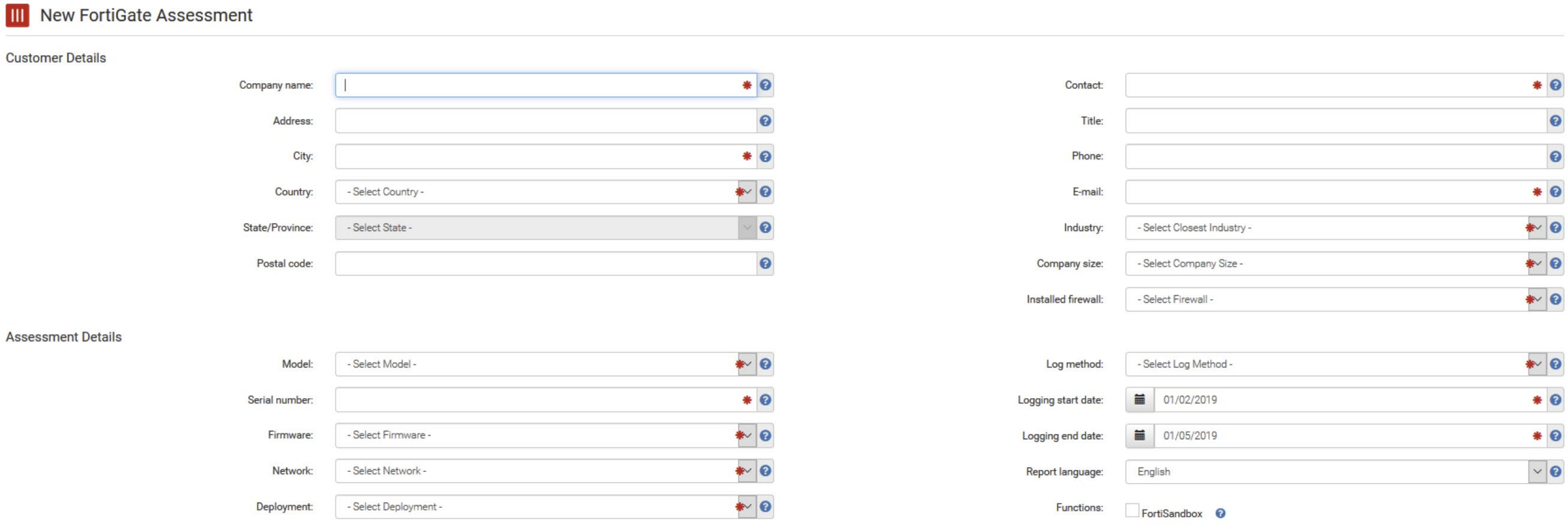
It was originally sent by Loan Request (Exclusive Networks) to loanapprovalsales@exclusive-networks.com.

Loan Request (Exclusive Networks) originally wrote:
"Please review and complete Fortinet Loan Agreement for EVO Ltd."

Click here to review and sign **Fortinet Loan Agreement**

NOTE: Please speak to your account manager to obtain a loan agreement form, check availability of CTAP unit, reserve and agree date for shipment.

Fortinet CTAP Portal



New FortiGate Assessment

Customer Details

Company name:		Contact:	
Address:		Title:	
City:		Phone:	
Country:	- Select Country -	E-mail:	
State/Province:	- Select State -	Industry:	- Select Closest Industry -
Postal code:		Company size:	- Select Company Size -
		Installed firewall:	- Select Firewall -

Assessment Details

Model:	- Select Model -	Log method:	- Select Log Method -
Serial number:		Logging start date:	01/02/2019
Firmware:	- Select Firmware -	Logging end date:	01/05/2019
Network:	- Select Network -	Report language:	English
Deployment:	- Select Deployment -	Functions:	□ FortiSandbox

The Cyber Threat Assessment Program Portal (https://ctap.fortinet.com) is a centralized tool for managing and tracking assessments. Once the serial number of the loan unit is known and the dates agreed to install and run the CTAP the Fortinet CTAP portal configuration can be setup.

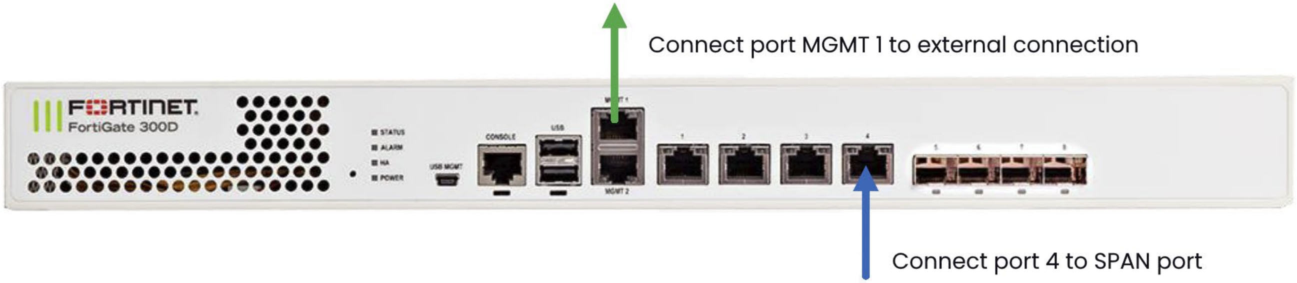
Information needed to configure the portal includes:

- Company name, industry, size, existing firewall vendor
- Fortigate serial number, firmware version (latest is installed on units)
- Start and end dates for assessment.

NOTE: The end date will trigger the generation of the CTAP report and the logging of traffic will stop after this date.

Installation of FortiGate CTAP unit 1 / 2

- Check with the customer that they have created the SPAN port on their switch, they need to span traffic destined for the inbound and outbound to the internet.
- Customer also needs to provide you with an IP address, Subnet Mask and Gateway



Connect port MGMT 1 to external connection

Connect port 4 to SPAN port

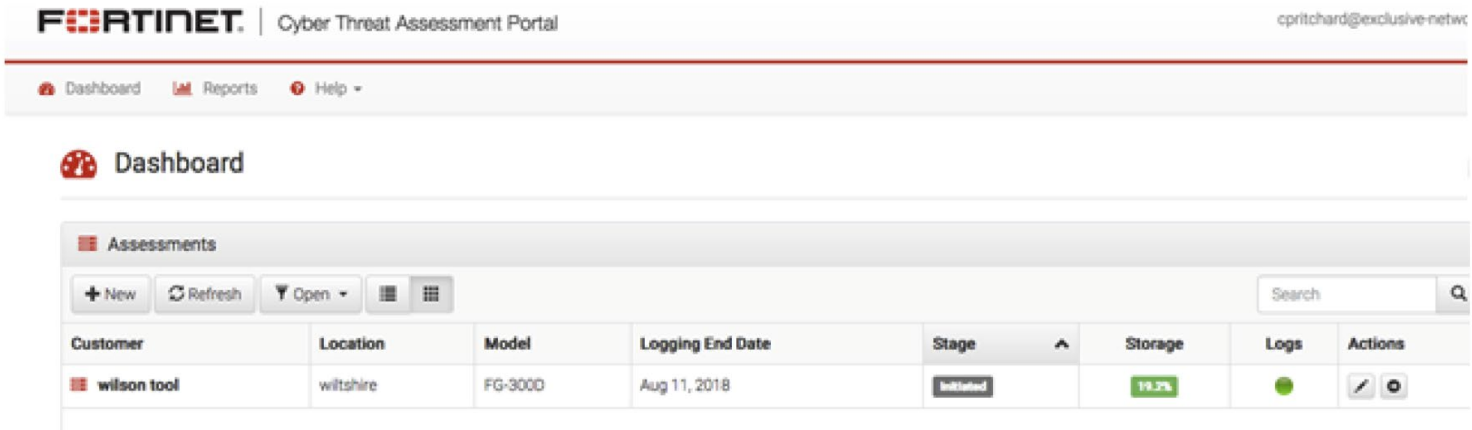
- Log into the CTAP unit using the MGMT1 port, and assign your laptop with an address of 192.168.1.1/24   GW 192.168.1.99
- Connect Port 4 to the customer switch
- Configure another port eg MGMT 2 with an IP address, subnet mask, I usually use 192.168.2.99/24 enable HTTPS access
- Disconnect your laptop from mgmt1 and connect it to mgmt2, change your laptop ip address to 192.168.2.1/24 GW 192.168.2.99
- Once connected to the GUI of the firewall, go to the Root VDOM, under network/interfaces open mgmt1 and assign the IP address and subnet mask supplied by the end user and switch off **"dedicated to management only"** then click apply
- From the GUI go to network, static routes and remove the static route.
- Add a new static route (GW provided by the end user) select interface mgmt1 and click apply
- From the console widget on the GUI ping 8.8.8.8 to confirm connectivity to the internet

Installation of FortiGate CTAP unit 2 / 2

- From the GUI in the root VDOM go to Logging and confirm logs are being received and you have connectivity to the FortiAnalyzer in the FortiGuard network

- If you cannot hit the FortiGuard network and logs are being queued you have a problem, most likely the end users firewall. If they have a Cisco ASA they may need to disable DNS Inspection

- Once you have connectivity, log back into the ctap portal https://ctap.fortinet.com and confirm logs are being received, the logs radio button should be Green and not Red, please note that it can sometimes take a few minutes for the radio button to turn green.


FORTINET | Cyber Threat Assessment Portal
cpritchard@exclusive-netwo
Dashboard
Reports
Help
Dashboard
Assessments
New
Refresh
Open
Search

Customer	Location	Model	Logging End Date	Stage	Storage	Logs	Actions
wilson tool	wiltshire	FG-300D	Aug 11, 2018	Initiated	19.2%	●	

CTAP Report

- At the end of the CTAP logging, ie the end date as set on the Fortinet CTAP portal has lapsed the CTAP report will be generated and an email sent out informing of the completion.

- The report can then be downloaded from the CTAP portal.

- The report should be analyzed and key points highlighted so that it can be presented to the end user in a concise and informative manner.

- **Present report back to end user.**

  - Please see the CTAP Portal help section for tutorials on presenting the report or to download materials on Interpreting the Report.

- **Agree next actions with the end user**,

  - i.e. how to correct the issues and improve their network security, improve productivity and proactively monitor network utilisation and associated risks.

- The CTAP unit can be uninstalled, packaged and returned to Exclusive Networks.

NOTE: It is the partners responsibility to ensure the FortiGate unit is uninstalled, placed back in its original packaging along with the appropriate cables (network, power cable) and returned back to Exclusive Networks.