cisco Live!

Let's go

The bridge to possible

Think Like a TAC Engineer

Troubleshooting Secure Client Remote Access Issues

Tomasz Kmiec, Security Technical Leader



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Introduction
- Remote Access Troubleshooting Methodology
- Troubleshooting Tools
- Common Issues
- Conclusion

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

About Your Speaker



Tomasz Kmiec

CISCO CERTIFIED CCIE SECURITY

Security Technical Leader, Cisco TAC

- Based in Krakow, Poland
- Working in TAC since March 2017
- Focusing on VPN and NGFW solutions
- Enjoy cycling, working out and traveling



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Webex App

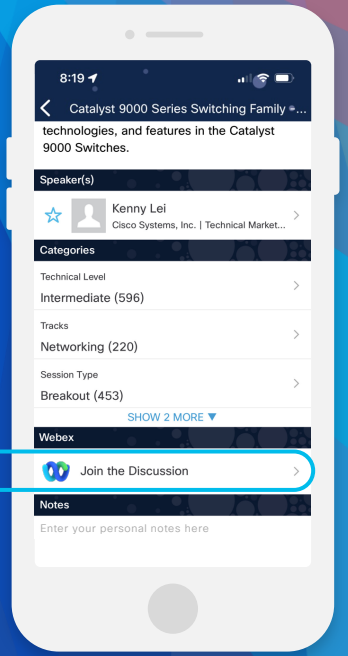
Questions?

Use the Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

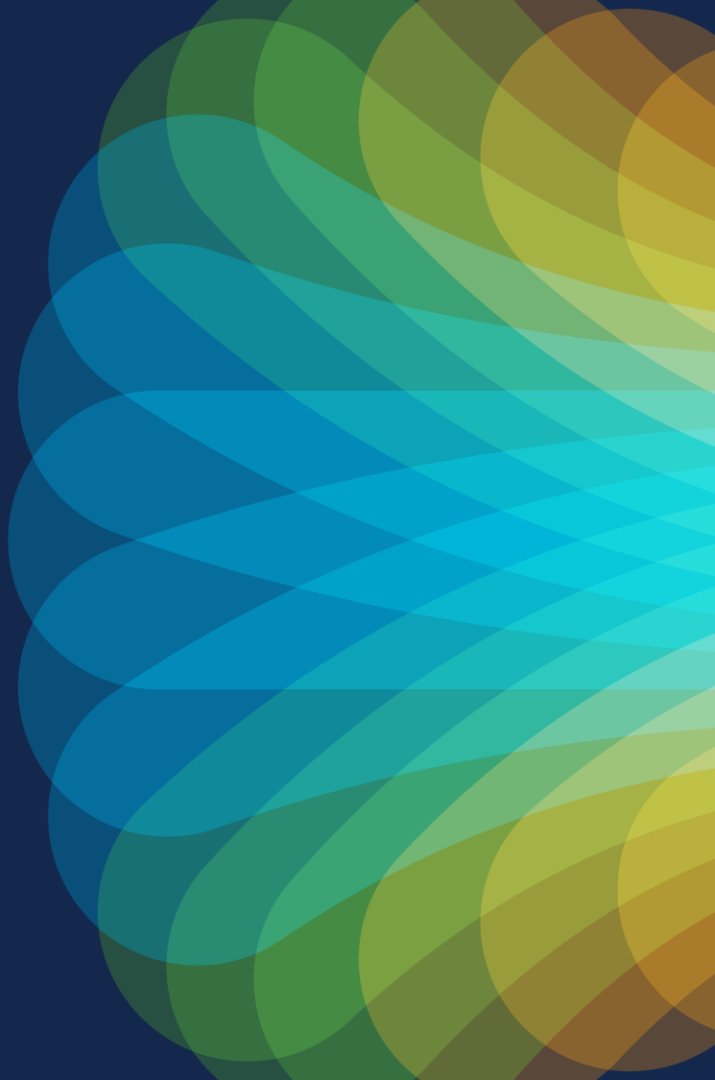
Webex spaces will be moderated by the speaker until February 23, 2024.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-3935

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Introduction



Introduction

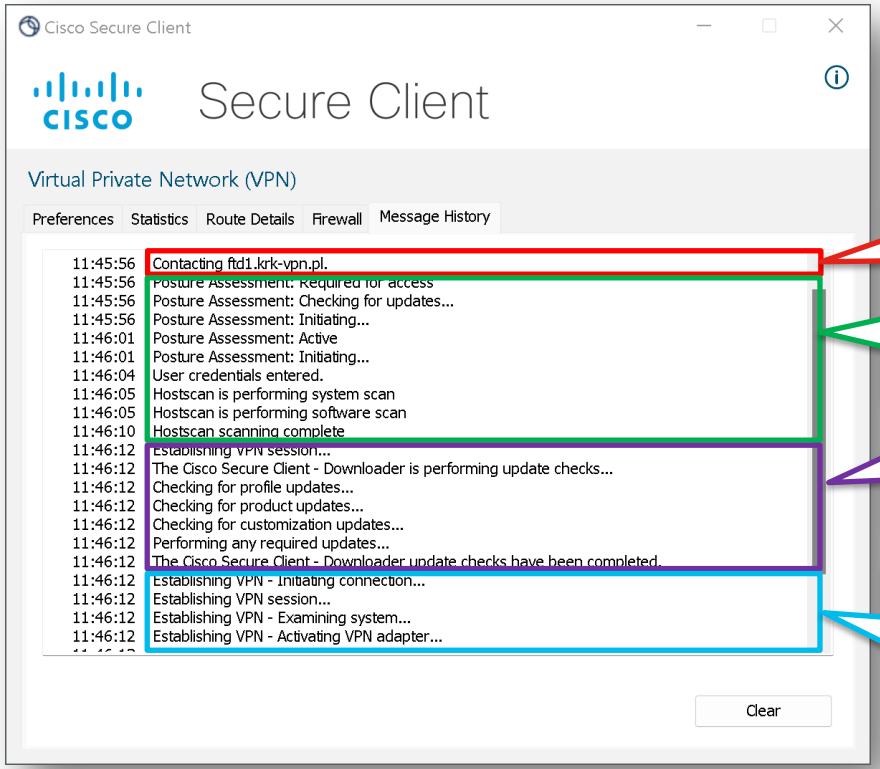
This session covers troubleshooting tools, methodology, and real examples that are coming from TAC Service Requests.

This session doesn’t cover configuration or feature introduction.

During this session, we will be going through the Secure Client Remote Access Connection Flow.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Client Remote Access Connection Flow



Establishing TLS or IKEv2 session

Authentication
Group-policy assignment
HostScan (optional)

Client services

Tunnel establishment

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Remote Access Troubleshooting Methodology

Where to Start?

The key objective is to narrow down the problem to one of the following:

- Control plane; connectivity issues, TLS handshake, authentication, authorization, session disconnects, etc.,

- Data plane; traffic not flowing or impacted.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

“A Problem Well-Defined is a Problem Half-Solved”

Charles Kettering

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Define the problem

Isolate the problem

Find a solution

- When did the problem start?
- Is it a working setup or a new implementation?
- Any changes?
- What are the symptoms?
- Who is affected?

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Define the problem

Isolate the problem

Find a solution

- Control plane or data plane issue?
- Affected platforms?
- Any known trigger?
- Does the location matter?

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Define the problem

Isolate the problem

Find a solution

- Any changes on integrated components?
- Is the connection to another headend working properly?
- Which application/traffic is affected?

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Define the problem

Isolate the problem

Find a solution

- Check the documentation and release notes.
- Collect and analyze data.
- Check Cisco Forum, Google.
- Check Bug Search Tool.
- Contact TAC.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Problem Description Is a Key!

Secure Client it's not working.

Vague description, no details.

Secure Client RA VPN sessions cannot be established by **random users** from **various locations**. **Multiple platforms** are affected. The authentication method is **SAML**.

After providing credentials, the following error is displayed: **Authentication failure**.

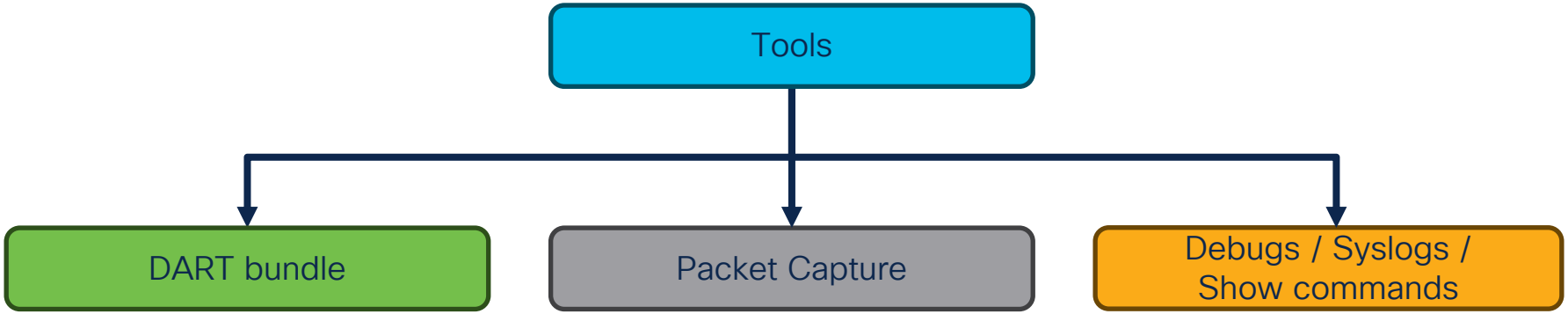
The issue is **intermittent**. **No recent changes** on the FTD side and in the network environment.
Local user authentication works fine.

Problem description includes a lot of details about the issue.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Troubleshooting Tools

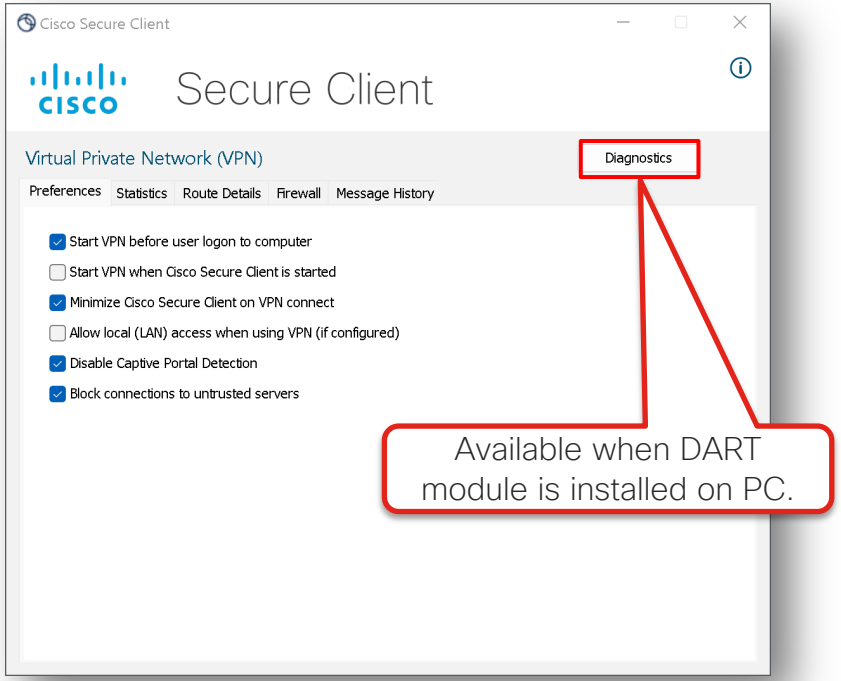
Troubleshooting Tools for Remote Access VPN

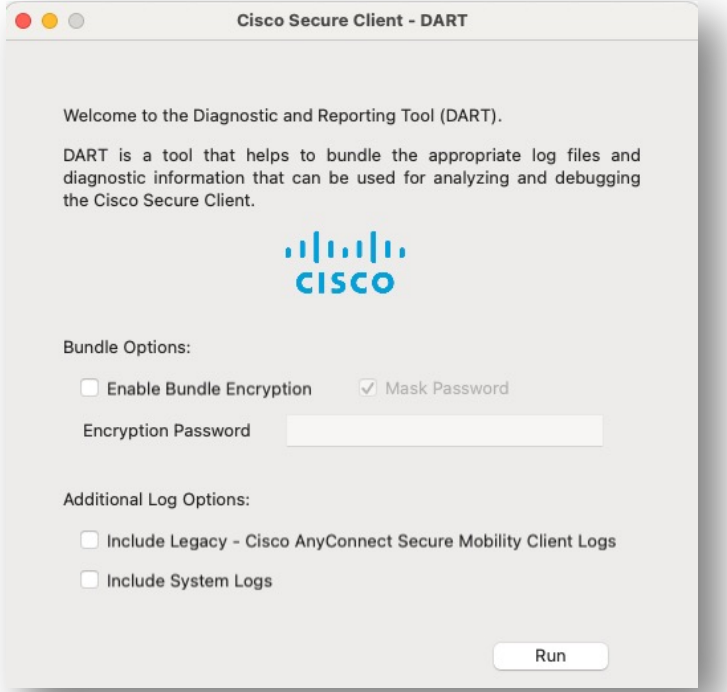


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

DART Bundle – Crucial Logs in RAVPN Troubleshooting

- DART is the Secure Client (AnyConnect) Diagnostics and Reporting Tool to collect data for troubleshooting RAVPN installation and connection problems.

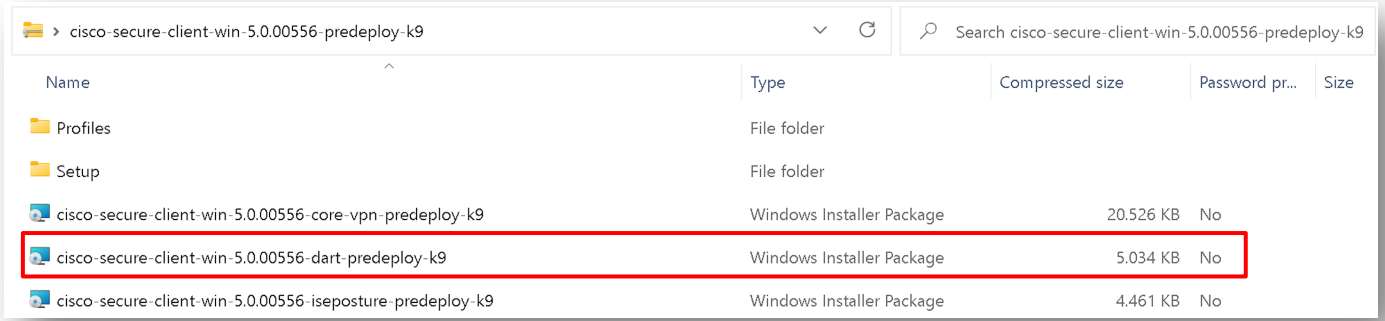




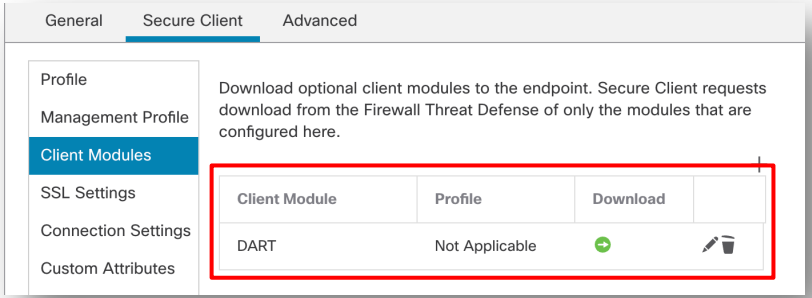
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

DART Module Installation

- The DART can be installed manually using the **msi** file included in the the pre-deploy package:



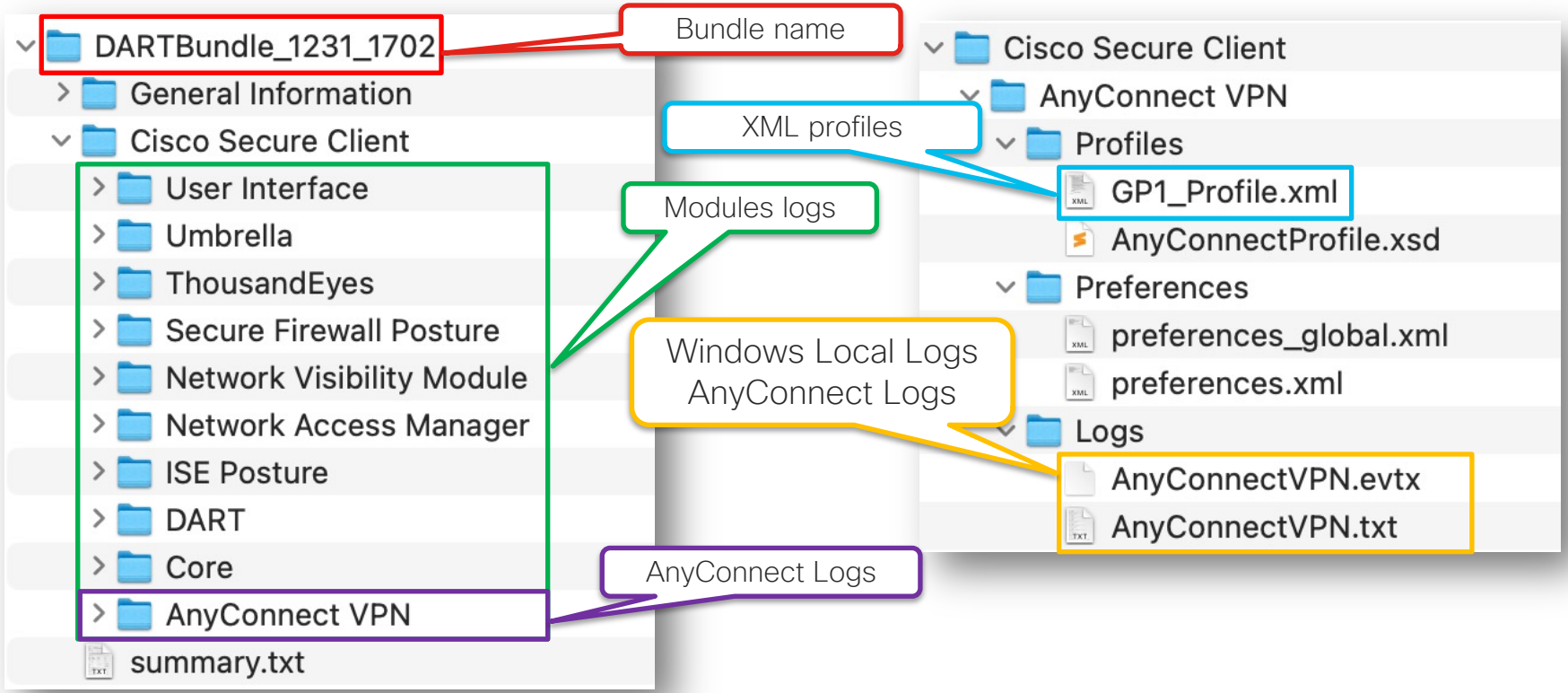
- The other option is enabling DART module configuration under the Group Policy:




```
ASA# show run group-policy GP1
group-policy GP1 attributes
 [..]
 webvpn
  anyconnect keep-installer none
  anyconnect modules value dart
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Reviewing DART Bundle Content



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

DART Bundle Key Log Messages (AnyConnectVPN.txt)

```
Description : An SSL VPN connection to ftd1.krk-vpn.pl has been requested by the user
Resetting client certificate list.
Number of certificates found: 3
```

Establishing TLS or IKEv2 session

```
Authentication is not token based (OTP)
User submitted response for host ftd1.krk-vpn.pl and tunnel group: RAVPN1
Authentication succeeded (SSL) / Authentication is complete (IKEv2).
```

Authentication

```
Description : The profile configured on the secure gateway is: GP1_Profile.xml
The Cisco Secure Client - Downloader is performing update checks...
Description : Initiating VPN connection, Cisco Secure Client - AnyConnect VPN version 5.0.05040
```

Client services

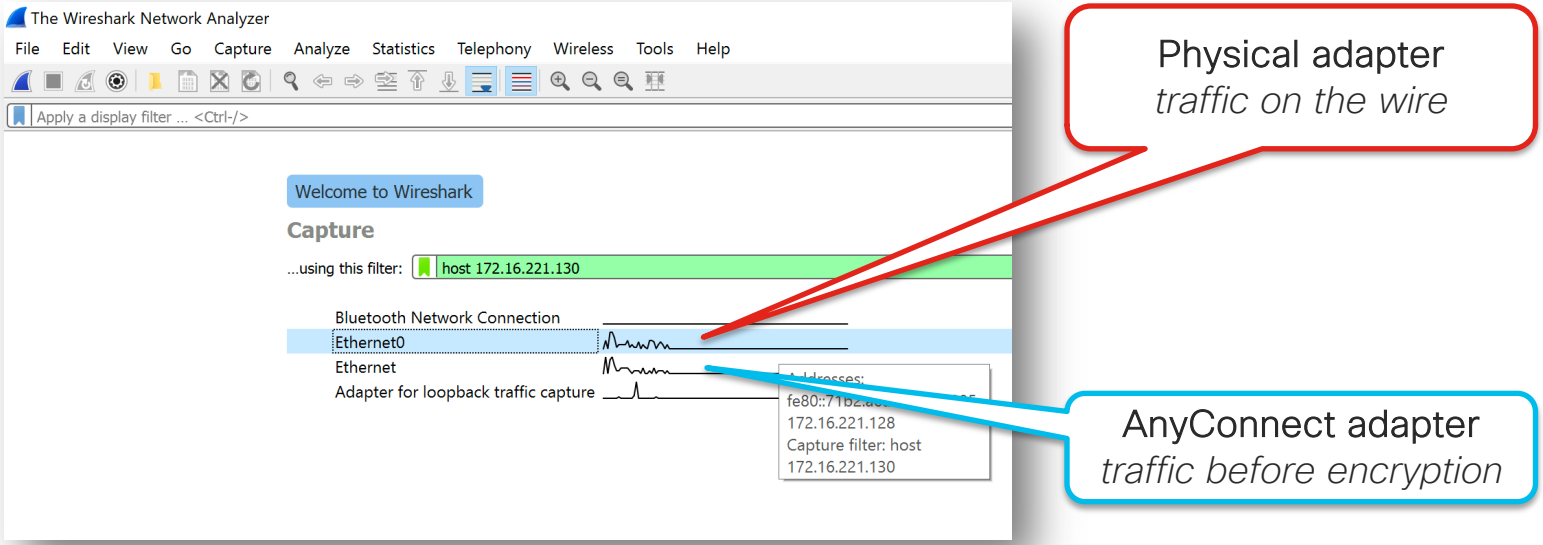
```
Description : The Primary SSL connection to the secure gateway is being established.
Description : A TLS 1.3 connection has been established using cipher TLS_AES_128_GCM_SHA256
Establishing VPN - Examining system..
Establishing VPN - Activating VPN adapter...
Establishing VPN - Configuring system...
Description : The VPN connection has been established and can now pass data.
Connected to ftd1.krk-vpn.pl
Description : The Primary DTLS connection to the secure gateway is being established.
Description : The Primary DTLS connection to the secure gateway has been established.
```

Tunnel establishment

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Packet Capture on Host

Packet capture can be enabled on the host machine to check the packet flow:



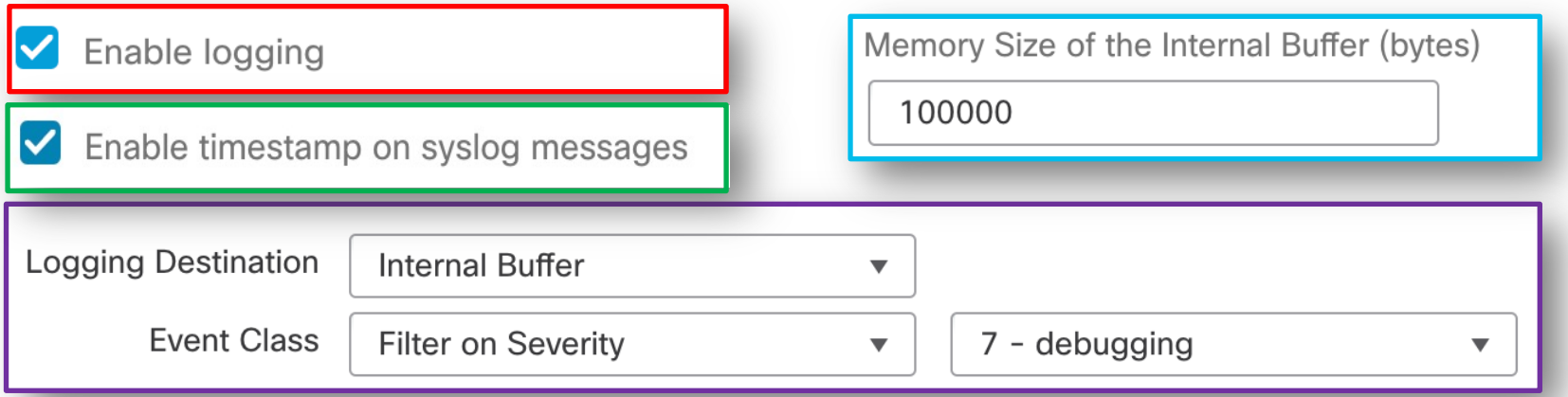
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Syslog Messages on the Headend

- Syslog messages are very valuable but very often forgotten
- On the ASA, logging can be configured via CLI or ASDM

```
ASA(config)# logging enable
ASA(config)# logging timestamp
ASA(config)# logging buffer-size 100000
ASA(config)# logging buffered informational
```

- On the FTD, logging can be configured in the Platform Settings:



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Syslog Messages – Logging Buffered

```
firepower# show logging

Jan 20 2024 21:54:00: %FTD-6-725001: Starting SSL handshake with client
outside:10.48.17.29/56337 to 10.48.30.163/443 for TLS session
Jan 20 2024 21:54:00: %FTD-7-725010: Device supports the following 3 cipher(s)
Jan 20 2024 21:54:00: %FTD-7-725011: Cipher[1] : TLS_AES_[illegible]_GCM_SHA256
Jan 20 2024 21:54:00: %FTD-7-725011: Cipher[2] : TLS_CHACHA[illegible]
Jan 20 2024 21:54:00: %FTD-7-725011: Cipher[3] : TLS_AES_2[illegible]
[..]
Jan 20 2024 21:54:00: %FTD-7-725012: Device chooses cipher
TLS_AES_128_GCM_SHA256 for the SSL session with client
outside:10.48.17.29/56337 to 10.48.30.163/443
Jan 20 2024 21:54:00: %FTD-6-725016: Device selects trust[illegible]point ftd1.krk-
vpn.pl for client outside:10.48.17.29/56337 to 10.48.30.163/443
Jan 20 2024 21:54:00: %FTD-6-725002: Device completed SSL handshake with
client outside:10.48.17.29/56337 to 10.48.30.163/443 for TLSv1.3 session
```

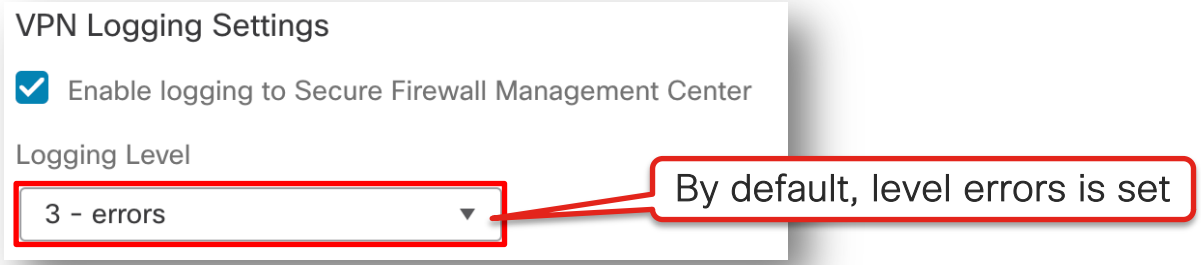
Starting TLS handshake

TLS handshake completed

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

VPN Logging to Secure Firewall Management Center

- VPN logging to Secure Firewall Management Center is enabled by default.



- Logs are seen under Devices -> VPN -> Troubleshooting:

Table View of VPN Troubleshooting

	Time	Severity	Message	Message Class	Username	Device
▼	2024-01-20 17:41:54	Error	Failed to consume SAML assertion. reason: The profile cannot verify a signature on the message.	WebVPN and AnyConnect Client		FTD1

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Reference

Syslog Messages – Key Points

- Enable timestamp for Syslog messages
- Use Network Time Protocol (NTP) to sync the clock between all devices that are debugged
- Use Syslog debugging level only when necessary
- Configure and verify if Syslog messages are sent and received on the external syslog server
- For FMC Syslog messages, don’t use informational or debug level if not necessary

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Debugs

- Debug messages help with verifying how the feature works, and in case of failure, what is the root cause.

Debugs are printed on ssh/console by default

```
firepower# debug webvpn anyconnect 255
Validating the session cookie...
Processing CSTP header line:
'webvpn=665ED7@172032@355A@E3A41B15E34795BFEA4068F7873C19F3D4B79518'
Found WebVPN cookie:
'webvpn=665ED7@172032@355A@E3A41B15E34795BFEA4068F7873C19F3D4B79518'
WebVPN Cookie:
'webvpn=665ED7@172032@355A@E3A41B15E34795BFEA4068F7873C19F3D4B79518'
Cookie validation successfull, session authenticated
http_parse_cstp_method()
...input: 'Host: ftd1.krk-vpn.pl'
Processing CSTP header line: 'Host: ftd1.krk-vpn.pl'
firepower# un all
```

Debugs should be disabled after necessary data is collected

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Debugs

- After closing the session, debugs are not printed unless the persistent option is configured:

```
ASA(config)# logging debug-trace persistent
```

- Option ‘logging debug-trace’ (ASA) or ‘Send debugs messages as syslogs’ (FMC) allows to redirect debugs to syslog destinations:

```
firepower# debug webvpn anyconnect 255
INFO: 'logging debug-trace' is enabled. All debug messages are currently being
redirected to syslog:711001 and will not appear in any monitor session
INFO: debug webvpn anyconnect enabled at level 255



firepower# show logging
Jan 13 2024 16:44:50: %FTD-7-711001: Validating the session cookie...
Jan 13 2024 16:44:50: %FTD-7-711001: Processing CSTP header line:
'webvpn=1FA719@167936@CF6E@3633AFE08A055A612EA3B3EF9CDB2B91BB24BCDF'
Jan 13 2024 16:44:50: %FTD-7-711001: Found WebVPN cookie:
'webvpn=1FA719@167936@CF6E@3633AFE08A055A612EA3B3EF9CDB2B91BB24BCDF'
```

The messages are generated on debugging level

Syslog messages instead of debugs

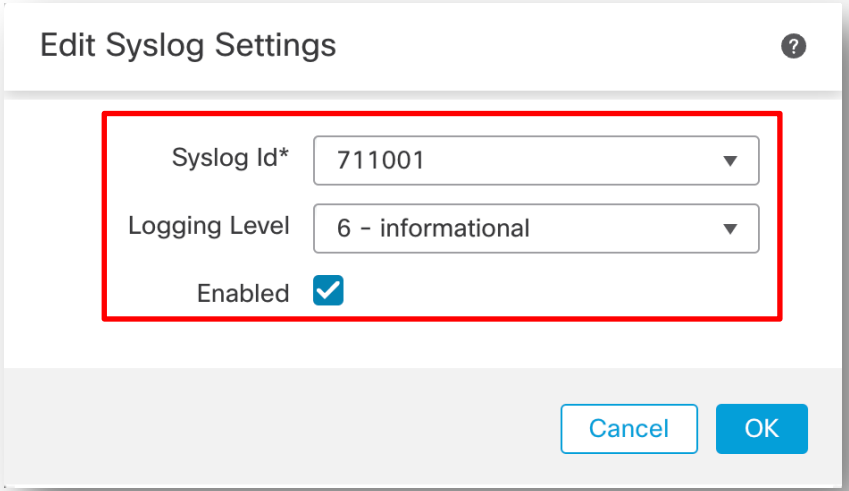
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Reference

Debugs as Syslogs

- If syslog settings cannot be configured on debugging level, severity of message 711001 can be changed:

```
ASA(config)# logging message 711001 level informational
```



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Reference

Useful Debugs for RAVPN Troubleshooting

AnyConnect/WebVPN

```
debug webvpn 255
debug webvpn anyconnect 255
```

IKEv2/IPSec

```
debug crypto condition peer X.X.X.X
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
```

DHCP

```
debug dhcpc detail 255
debug dhcpc error 255
debug dhcpc packet 255
```

AAA

```
debug aaa shim 255
debug ldap 255
debug radius all
debug webvpn saml 255
debug aggregate-auth ssl 255
debug aggregate-auth xml 255
debug aaa comm 128
```

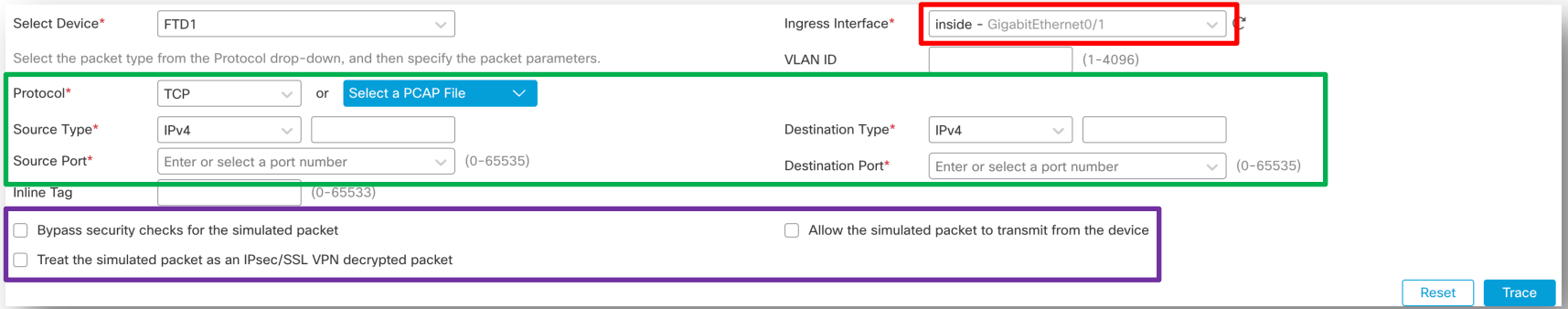
PKI

```
debug crypto ca 14
debug crypto ca scep-proxy 255
debug crypto ca trustpool 255
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Packet Tracer

- The Packet tracer allows to inject virtual packet into the device and checks how it is being processed.
- This tool can be initiated from FMC, ASDM and CLI:




```
firepower# packet-tracer input <ingress_interface> <protocol>
<src_IP> <src_port> <dst_IP> <dst_port> <option>
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Packet Tracer

```
firepower# packet-tracer input inside tcp 192.168.1.100 12345 172.16.1.10 12345 detailed
```

Ingress Interface

Protocol

Src_IP Src_Port Dst_IP Dst_Port

Option

```
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Elapsed time: 11675 ns
Config:
nat (inside,outside) source static IPv4-Private-192.168.0.0-16 IPv4-Private-
192.168.0.0-16 destination static NET-172.16.1.0 NET-172.16.1.0 no-proxy-arp
Additional Information:
NAT divert to egress interface outside(vrfid:0)
Untranslate 172.16.1.10/12345 to 172.16.1.10/12345
```

Component

Result

Applied configuration

Additional Information

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Packet Tracer

Reference

```
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Elapsed time: 2521 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434432 event-log flow-
end
access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: ACP1 - Default
access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be
reached
 Forward Flow based lookup yields rule:
 in  id=0x14bfa4c4fce0, priority=12, domain=permit, deny=false
       hits=219930, user_data=0x14bf4b6e22c0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Packet Tracer

Reference

```
Phase: 10
Type: WEBVPN-SVC
Subtype: out
Result: ALLOW
Elapsed time: 24751 ns
Config:
Additional Information:
 Forward Flow based lookup yields rule:
 out id=0x14bfa73aa860, priority=71, domain=svc-ob-tunnel-flow, deny=false
      hits=2, user_data=0x31000, cs_id=0x0, reverse, flags=0x0, protocol=0
      src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
      dst ip/id=172.16.1.10, mask=255.255.255.255, port=0, tag=any
```

```
Phase: 19
Type: SNORT
Subtype: firewall
Result: ALLOW
Elapsed time: 50266 ns
Config:
Network 0, Inspection 0, Detection 3, Rule ID 268434432
Matched rule ids 268434432 - Trust
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Packet Tracer

Reference

```
Phase: 21
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Elapsed time: 7005 ns
Config:
Additional Information:
Found next-hop 10.48.30.1 using egress ifc  outside(vrfid:0)
```

```
Result:
input-interface: inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 226153 ns
```

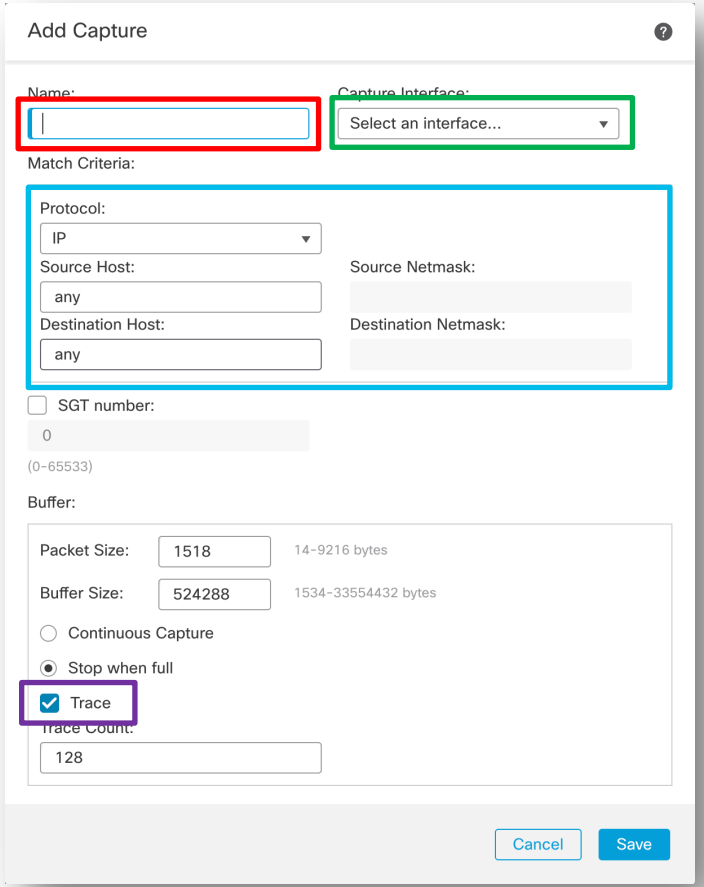

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Packet Capture

- Packet capture can be initiated from the CLI or the device manager (ASDM or FMC)

- It allows to check if packet is reaching and leaving the device in the expected way

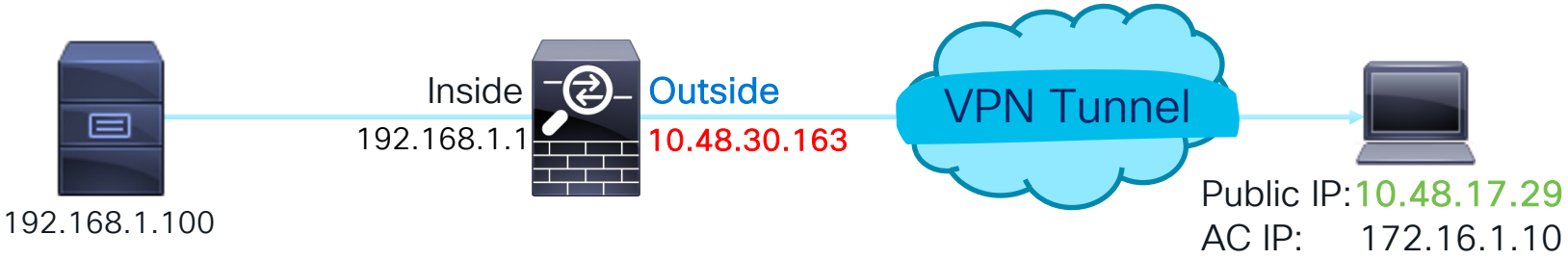
```
ASA# capture <capture name> interface
<interface name> match <conditon>
<option>
```



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Capture Points on the Headend

Capturing encrypted traffic between client and ASA/FTD on Outside interface.




```
FTD# capture cap1 interface Outside match ip host 10.48.30.163 host 10.48.17.29
```

```
FTD# show cap cap1

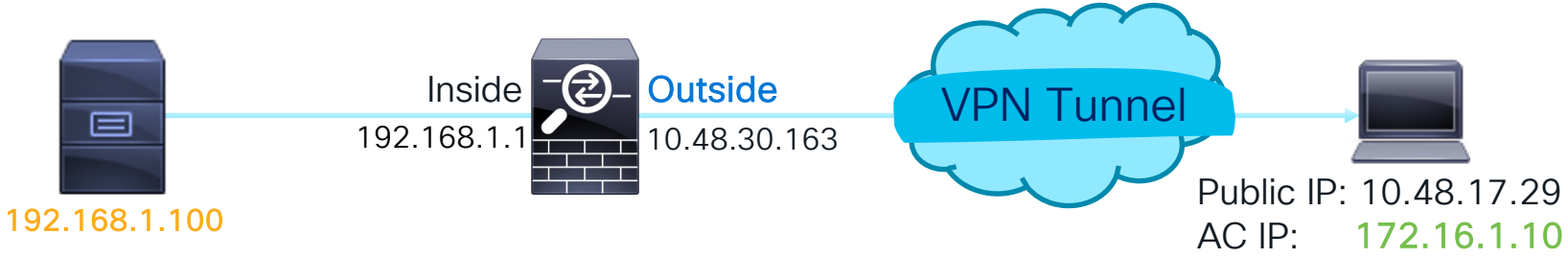
   1: 15:13:48.624540       10.48.17.29.51856 > 10.48.30.163.443:  udp 98
   2: 15:13:48.626676       10.48.30.163.443 > 10.48.17.29.51856:  udp 98
   3: 15:13:49.641690       10.48.17.29.51856 > 10.48.30.163.443:  udp 98
   4: 15:13:49.652462       10.48.30.163.443 > 10.48.17.29.51856:  udp 98
```

2-way communication
(TLS/DTLS/ESP)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Capture Points on the Headend

Capturing real traffic between server and client on Outside interface.




```
FTD# capture cap2 interface Outside match ip host 192.168.1.100 host 172.16.1.10
FTD# capture cap2 include-decrypted
```

```
FTD# show cap cap2

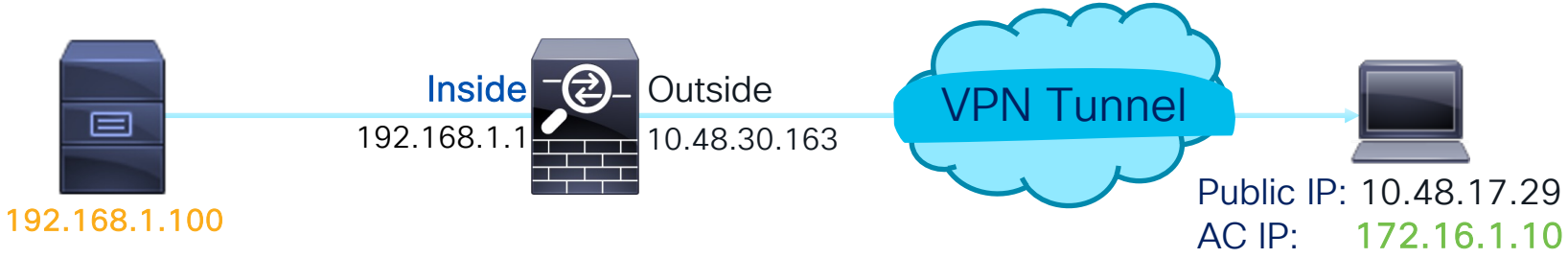
   1: 15:13:48.624601       172.16.1.10 > 192.168.1.100 icmp: echo request
   2: 15:13:49.641766       172.16.1.10 > 192.168.1.100 icmp: echo request
```

1-way communication
(only decrypted packets from client)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Capture Points on the Headend.

Capturing real traffic between server and client on Inside interface




```
FTD# capture cap3 interface Inside match ip host 192.168.1.100 host 172.16.1.10
```

```
FTD# show cap cap3

   1: 15:13:48.624769       172.16.1.10 > 192.168.1.100 icmp: echo request
   2: 15:13:48.626615       192.168.1.100 > 172.16.1.10 icmp: echo reply
   3: 15:13:49.641904       172.16.1.10 > 192.168.1.100 icmp: echo request
   4: 15:13:49.652325       192.168.1.100 > 172.16.1.10 icmp: echo reply
```

2-way communication

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Reference

Useful Options for Packet Capture

- **trace** – provides a packet-tracer output for captured packets
- **include-decrypted** – include IPSec/SSL VPN decrypted packets in the capture (inbound traffic only)
- **type isakmp** - capture encrypted IKE payloads and decrypt it
- **type asp-drop** - allows to capture packets with specific drop reason

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Show Outputs

- The 'show outputs' help verify how feature works on the device.
- Outputs can be collected via CLI or device manager (FMC, ADSM):




```
ASA# show vpn-sessiondb
```

All outputs are avaliable from diagnostic-cli

```
> system support diagnostic-cli
firepower# show vpn-sessiondb
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Reference

Useful Show Commands for RAVPN Troubleshooting

VPN session

```
show vpn-sessiondb anyconnect
show vpn-sessiondb detail anyconnect
show ip local_pool
```

IKEv2/IPSec session

```
show crypto ikev2 sa
show crypto ipsec sa
```

AAA

```
show aaa-server
show saml metadata
show uauth
```

PKI

```
show crypto ca certificate
show crypto ca trustpoint
```

TLS

```
show ssl
show ssl ciphers
show ssl errors
```

Syslogs/Debugs

```
show logging buffer
show debug
```

Platform/System

```
show asp drop
show counters
system support trace
```

Packet Flow

```
show nat
show route
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

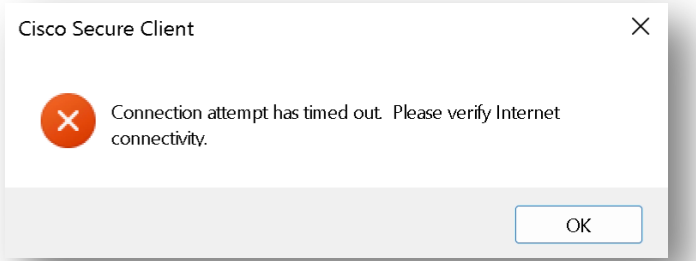
Common Issues

Issue #1

Reported problem: Users cannot establish RAVPN session.

Detailing:

- Only a few users affected, multiple OS
- Users can connect to the different headend
- The issue started without a known trigger



Triage: Control plane issue, most likely connectivity problem between host and headend

Action plan:

- Collect the DART bundle to confirm a failure reason
- Collect captures on the client and FTD

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #1

Investigation:

Connection timed out

1. DART bundle (AnyConnectVPN.txt):

```
****************************************
CURL error: 28 = Connection timed out after 8014 milliseconds

Message type error sent to the user:
Connection attempt has timed out.  Please verify Internet connectivity.
****************************************
```

No response for TCP SYN packets from client

2. Capture on host:

	Time	Source	Destination	Protocol	Lengt	Info
1	0.000000	10.48.17.29	10.48.30.163	TCP	66	49952 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2	1.020427	10.48.17.29	10.48.30.163	TCP	66	[TCP Retransmission] 49952 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
3	3.033335	10.48.17.29	10.48.30.163	TCP	66	[TCP Retransmission] 49952 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
4	7.042816	10.48.17.29	10.48.30.163	TCP	66	[TCP Retransmission] 49952 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460

3. Capture on headend:

```
firepower# capture capo interface outside match tcp host 10.48.17.29 host 10.48.30.163
firepower# show cap capo
0 packet captured
```

TCP SYN packets not seen on the FTD

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #1

Results:

- The issue has been isolated: **packet drop between the client and the FTD.**
- As a next step, packet capture should be collected on devices between the client and FTD to find at which stage packets are dropped.

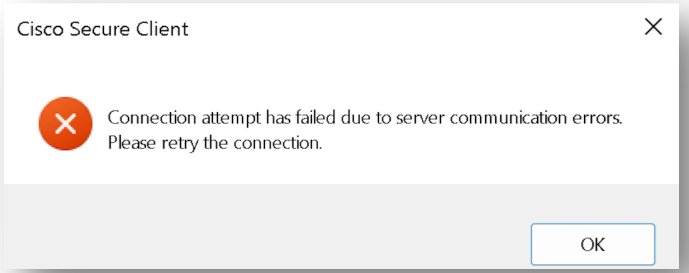
Note: IKEv2 sessions are blocked much more often than TLS sessions. If you are seeing similar symptoms for IKEv2 sessions, enable packet capture and check if there is any packet drop between the headend and the remote client.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #2

Reported problem: Users cannot establish RAVPN session.

Detailing:



- Multiple users affected, different OS
- Affected version: 4.10.x and 5.0.0
- Users with version 5.0.5 can connect
- There were changes on the firewall, but admin is unreachable

Triage: Control plane issue, additional data is needed to confirm the failure reason

Action plan:

- Collect the DART bundle to confirm a failure reason
- Check Syslog messages
- Collect captures on the client and FTD

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #2

Investigation:

SSL connection errors

1. DART bundle (AnyConnectVPN.txt):

```
****************************************
CURL error: 35 = error:1409442E:SSL routines:ssl3_read_bytes:tlsv1 alert protocol
version

35 : SSL connect error

Connection attempt has failed due to server communication errors. Please retry the
connection.
****************************************
```

2. Capture on host:

Protocol version error

	Time	Source	Destination	Protocol	Lengt	Info
1	0.000000	10.48.17.29	10.48.30.163	TCP	66	50166 → 443 [SYN] Seq=
2	0.000680	10.48.30.163	10.48.17.29	TCP	60	443 → 50166 [SYN, ACK] Seq=0 …32768 Len=0 MSS=1380
3	0.000735	10.48.17.29	10.48.30.163	TCP	54	50166 → 443 [ACK] Seq=1 Ac… …64240 Len=0
4	0.001340	10.48.17.29	10.48.30.163	TLSv1…	235	Client Hello
5	0.001670	10.48.30.163	10.48.17.29	TCP	60	443 → 50166 [ACK] Seq=1 Ack=182 Win=32768 Len=0
6	0.001775	10.48.30.163	10.48.17.29	TLSv1…	61	Alert (Level: Fatal, Description: Protocol Version)

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #2

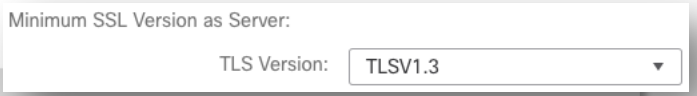
Investigation:

3. Syslog messages:

```
Jan 01 2024 19:42:58: %FTD-6-725001: Starting SSL handshake with client
outside:10.48.17.29/50166 to 10.48.30.163/443 for TLS session
Jan 01 2024 19:42:58: %FTD-7-725014: SSL lib error. Function:
tls_early_post_process_client_hello Reason: unsupported protocol
Jan 01 2024 19:42:58: %FTD-6-725006: Device failed SSL handshake with client
outside:10.48.17.29/50166 to 10.48.30.163/443
Jan 01 2024 19:42:58: %FTD-7-609002: Teardown local-host outside:10.48.17.29 duration
0:00:00
```

Unsupported protocol

4. TLS configuration on the headend:




```
firepower# show ssl
Accept connections using SSLv3 or greater and negotiate to TLSv1.3 or greater
Start connections using TLSv1.2 and negotiate to TLSv1.2 or greater
SSL DH Group: group14 (2048-bit modulus, FIPS)
SSL ECDH Group: group19 (256-bit EC)
```

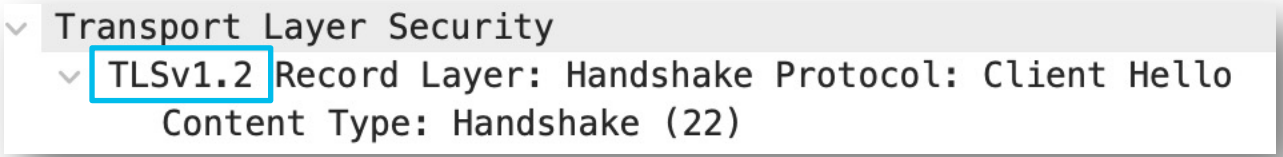
Only TLS1.3 sessions are accepted

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #2

Results:

- After analyzing the collected capture, it has been confirmed that the Secure Client is trying to establish a session using TLS 1.2:



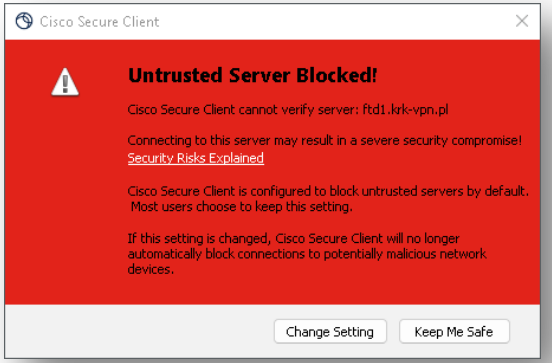
- As a solution, the TLS setting has been adjusted on the FTD to accept TLS 1.2 sessions, all clients upgraded to version that supports TLS 1.3, and then, TLS 1.3 was configured again on the headend.

Note: TLS 1.3 has been introduced on Secure Client 5.0.1.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #3

Reported problem: Users cannot establish the session.



Detailing:

- All users affected, multiple versions and OS
- A new certificate has been deployed

Triage: Control plane issue, certificate installed on FTD must be verified

Action plan:

- Check the certificate which is installed on FTD
- Use packet capture or OpenSSL for investigation
- DART bundle can be collected to confirm the failure reason

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #3

Errors point to untrusted source

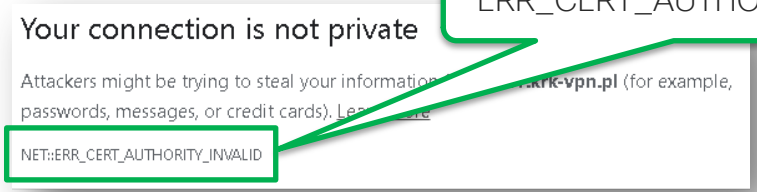
Investigation:

1. DART bundle (AnyConnectVPN.txt):

```
Description : Server certificate validation failed with the following errors:
     Certificate is from an untrusted source.
```

2. Web browser:

ERR_CERT_AUTHORITY_INVALID



3. OpenSSL allows to check the certificate details:

CA which issued certificate

```
HOST22~ % openssl s_client -connect 10.48.30.163:443 -showcerts
CONNECTED(00000004)
[..]
---
Certificate chain
 0 s:/C=pl/ST=malopolskie/L=krakow/O=tac/OU=cx/CN=ftd1.krk-vpn.pl
   i:/CN=ca.krk-vpn.pl
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #3

Results:

- It has been found that the CA Certificate was missing on the client.
- The issue was resolved by installing the missing CA certificate.

Note: If the identity certificate was issued by Sub CA, make sure that both certificates (root CA and subordinate CA) are installed on the host.

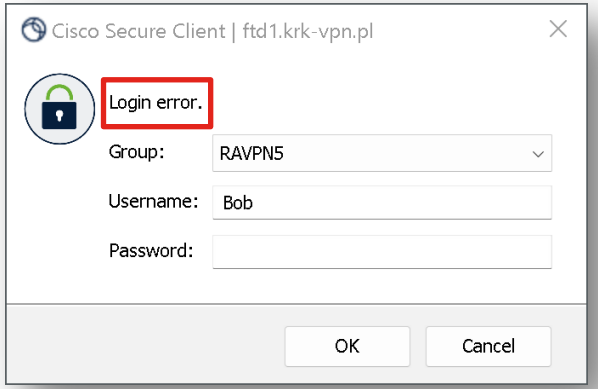
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #4

Reported problem: Users cannot establish RAVPN session.

Detailing:

- All users are affected
- Login error is displayed after providing credentials
- The issue started without a known trigger
- The authentication method is RADIUS



Triage: Control plane issue, communication with RADIUS has to be checked

Action plan:

- Check syslog and outputs, verify connectivity between FTD and AAA server
- DART bundle can be collected to confirm a failure reason

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #4

Investigation:

1. DART bundle (AnyConnectVPN.txt):

Logging error received from FTD

```
The following error message was received from the secure gateway:
Login error.
```

2. Syslog messages:

Syslogs point to the connectivity issue

```
Jan 23 2024 18:44:14: %FTD-6-113014: AAA authentication server not accessible :
server =  10.48.23.123 : user = *****
Jan 23 2024 18:44:14: %FTD-2-113022: AAA Marking RADIUS server 10.48.23.123 in aaa-
server group Radius-AAA as FAILED
```

3. Packet capture on FTD:

No response from RADIUS Server

```
1: 16:19:07.432869       10.48.30.163.23833 > 10.48.23.123.1812:  udp 744
2: 16:19:17.496708       10.48.30.163.23833 > 10.48.23.123.1812:  udp 744
3: 16:19:27.566773       10.48.30.163.23833 > 10.48.23.123.1812:  udp 744
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #4

Investigation:

4.Output ‘show aaa-server’:

```
Server Group:    Radius-AAA
Server Protocol: radius
Server Address:      10.48.2
Server port:     1812(authentication), 1813(
Server status:   FAILED, Last transaction at 18      04 UTC Tue Jan 23 2024
Number of pending requests          0
Average round trip time             0ms
Number of authentication requests   9
Number of authorization requests    0
Number of accounting requests       0
Number of retransmissions           0
Number of accepts                   0
Number of rejects                   0
Number of challenges                0
Number of bad authenticators        0
Number of timeouts                  9
Number of unrecognized responses    0
```

Server Status FAILED

Number of requests sent to the server

Timeouts marked for all requests

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #4

Results:

- All evidences are pointing to the communication failure between RADIUS server and headend.
- The issue has been resolved by correcting the internal routing.

Note: This is a very common scenario with almost all types of AAA server. It may be necessary to apply packet capture on multiple hops to identify where the traffic is being dropped.

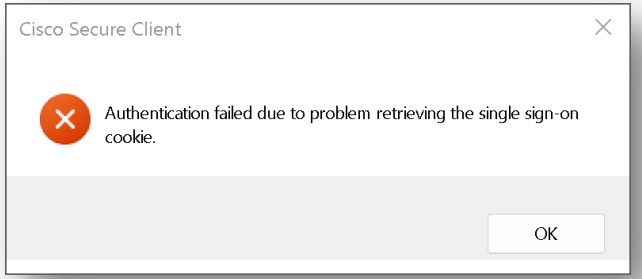
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #5

Reported problem: Users cannot establish RAVPN session.

Detailing:

- All users are affected
- Login error is displayed after providing credentials
- Issue started without a known trigger
- Authentication method is SAML



Triage: Control plane issue, communication with SAML IDP has to be checked

Action plan:

- Check syslog and enable SAML debugs if needed

*DART bundle may not be very helpful

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #5

Investigation:

DART may not include helpful logs when SAML authentication is failing

1. DART bundle (AnyConnectVPN.txt)

```
Processing user response.

Authentication failed due to problem retrieving the single sign-on cookie.
```

Log points to failure consume assertion

2. Syslog messages:

```
Jan 23 2024 19:21:11: %FTD-3-716162: Failed to consume SAML assertion. reason: The
identifier of a provider is unknown to #LassoServer. To register a provider in a
#LassoServer object, you must use the methods lasso_server_add_provider() or
lasso_server_add_provider_from_buffer()..
```

Debugs include the same reason

3. Debugs ‘debug webvpn saml 255’

```
Jan 23 19:21:11 [SAML] consume_assertion: The identifier of a provider is unknown
to #LassoServer. To register a provider in a #LassoServer object, you must use the
methods lasso_server_add_provider() or lasso_server_add_provider_from_buffer().
```

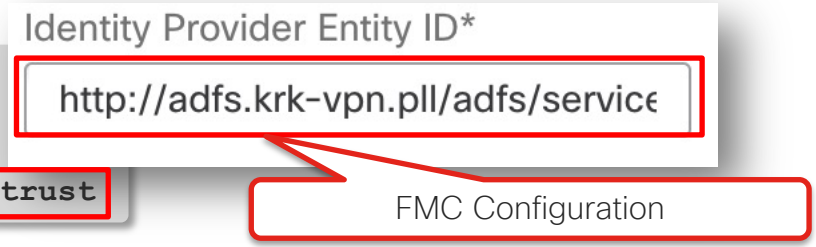

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #5

Results:

- This error indicates EntityID mismatch
- As a solution, EntityID has to be corrected in SAML IDP configuration:

```
firepower# show run webvpn
webvpn
 [..]
saml idp http://adfs.krk-vpn.pll/adfs/services/trust
```



Note: Most of SAML authentication issues can be identified by checking syslog messages and debugs (debug webvpn saml 255). In rare scenarios, https capture on the host is needed.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Common issues with SAML on ASA/FTD

Reference

The following debugs/syslog messages can be generated when SAML authentication is failing:

```
[SAML] consume_assertion: assertion is expired or not valid
```

Most likely time mismatch between ASA/FTD and SAML IDP

Solution: correct time/NTP on ASA/FTD and IDP.

```
[SAML] consume_assertion: The profile cannot verify a signature on the message
```

Missing IDP certificate on ASA/FTD

Solution: Enroll IDP certificate on ASA/FTD.

```
[SAML] consume_assertion: assertion audience is invalid
```

Missing IDP certificate on ASA/FTD

Solution: correct the Audience configuration on the IdP. It must match the ASA/FTD's Entity ID.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

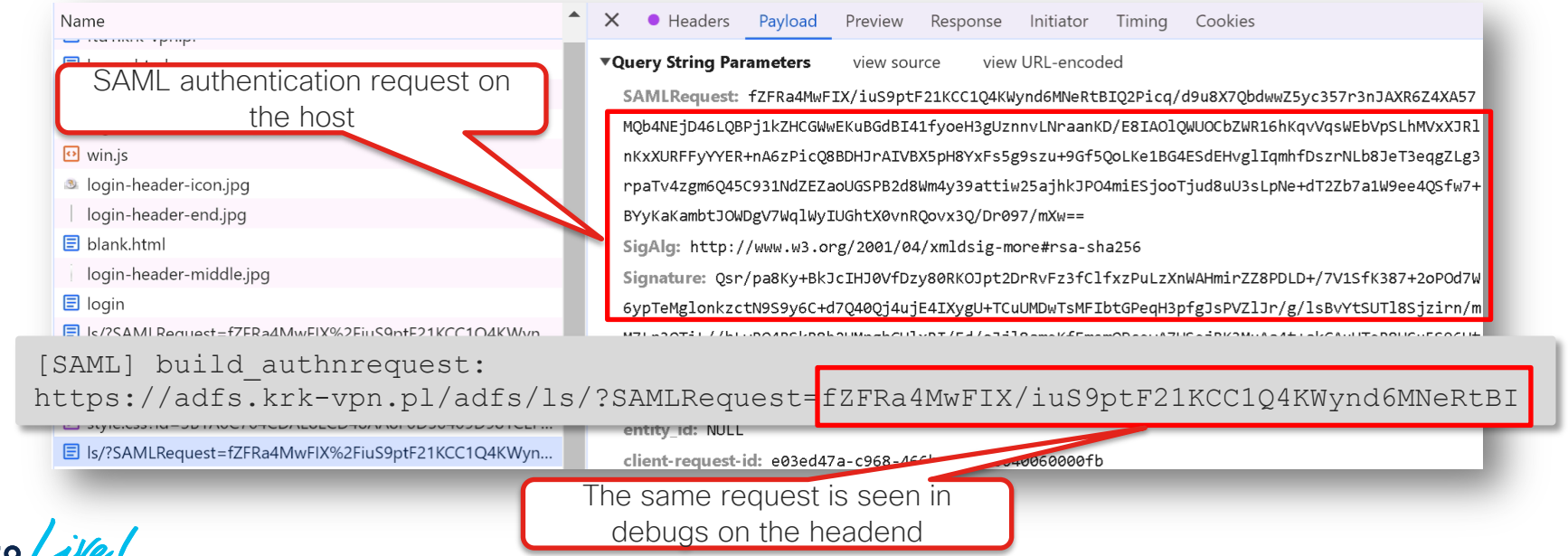
Common issues with SAML on ASA/FTD

Reference

If SAML debugs prints requests only, it could be either misconfiguration or an IDP issue.

Solution: Confirm base URL on ASA/FTD and make sure it's correct. Also, make sure that IDP is configured for the correct Assertion Consumer Service URL.

Note: There is an option to enable HTTPS capture on host:

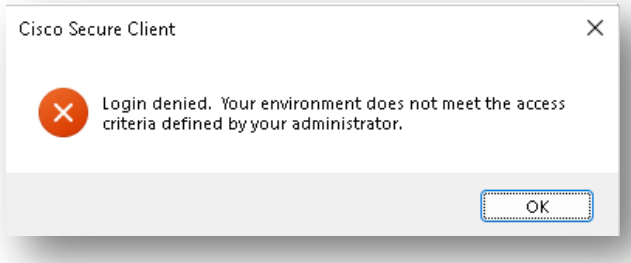


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #6

Reported problem: Users cannot establish RAVPN session.

Detailing:



- Issue reported by several but not all users.
- Login error is displayed after providing credentials
- The authentication method is RADIUS
- Dynamic Access Policy (DAP) has been implemented during the weekend.

Triage: Control plane issue, error points to DAP issue

Action plan:

- Collect ‘debug dap trace 255’ and then compare with the DAP configured on the device.

*DART bundle may not be very helpful

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #6

Investigation:

DART may not include helpful logs when DAP is failing

1. DART bundle (AnyConnectVPN.txt)

```
Login denied.  Your environment does not meet the access criteria defined by your
administrator.
```

2. DAP trace result:

User is hitting default rule

```
DAP_TRACE: Username: bob, Selected DAPs:
DAP_TRACE: dap_process_selected_daps: selected 0 records
DAP_TRACE: Username: bob, dap_aggregate_attr: rec_count = 1
DAP_TRACE: Username: bob, Selected DAPs: DfltAccessPolicy
DAP_TRACE: Username: bob, DAP_close: 33
```

Default Record: DfltAccessPolicy Terminate

3. DAP Configuration:

Anti-Malware (1 criterion)

Match criteria: All | Any

Type	Op.	Value
Real Time Scanning	=	true
Product Description	=	Cisco Advanced Malware Protection for Endpoints
Version	≥	7.1.6.11523

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #6

Investigation:

4. Debug dap trace 255:

Cisco AMP for Endpoints is detected

The version is 7.1.5.11523

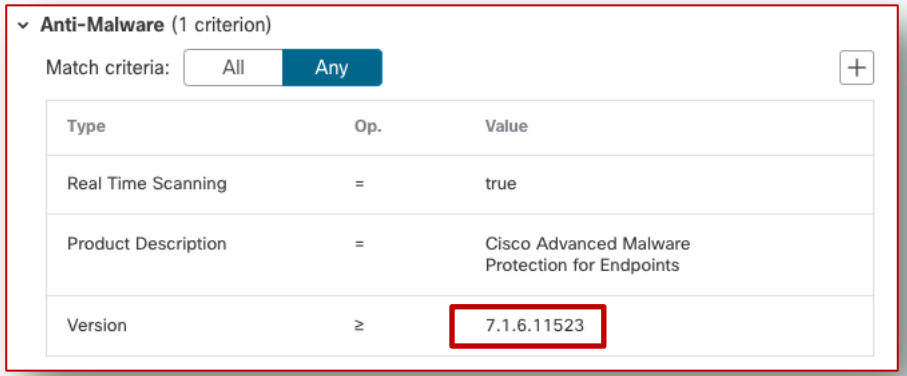
```
DAP_TRACE[128]:
dap_install_endpoint_data_to_lua:endpoint.am["2781"].description="Cisco Advanced
Malware Protection for Endpoints"
DAP_TRACE: endpoint.am["2781"].description = "Cisco Advanced Malware Protection
for Endpoints"
DAP_TRACE[128]:
dap_install_endpoint_data_to_lua:endpoint.am["2781"].version="7.1.5.11523"
DAP_TRACE: endpoint.am["2781"].version = "7.1.5.11523"
DAP_TRACE[128]:
dap_install_endpoint_data_to_lua:endpoint.am["2781"].activescan="ok"
DAP_TRACE: endpoint.am["2781"].activescan = "ok"
DAP_TRACE[128]:
dap_install_endpoint_data_to_lua:endpoint.am["2781"].lastupdate="1634128"
DAP_TRACE: endpoint.am["2781"].lastupdate = "1634128"
DAP_TRACE[128]:
dap_install_endpoint_data_to_lua:endpoint.am["2781"].timestamp="1704598254"
DAP_TRACE: endpoint.am["2781"].timestamp = "1704598254"
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #6

Results:

- According to DAP Policy, only hosts with AMP for Endpoint version equal or higher than 7.1.6.11523 are allowed to connect:



- However, the installed version is 7.1.5.11523.
- The issue was resolved by correcting the version in the DAP rule.

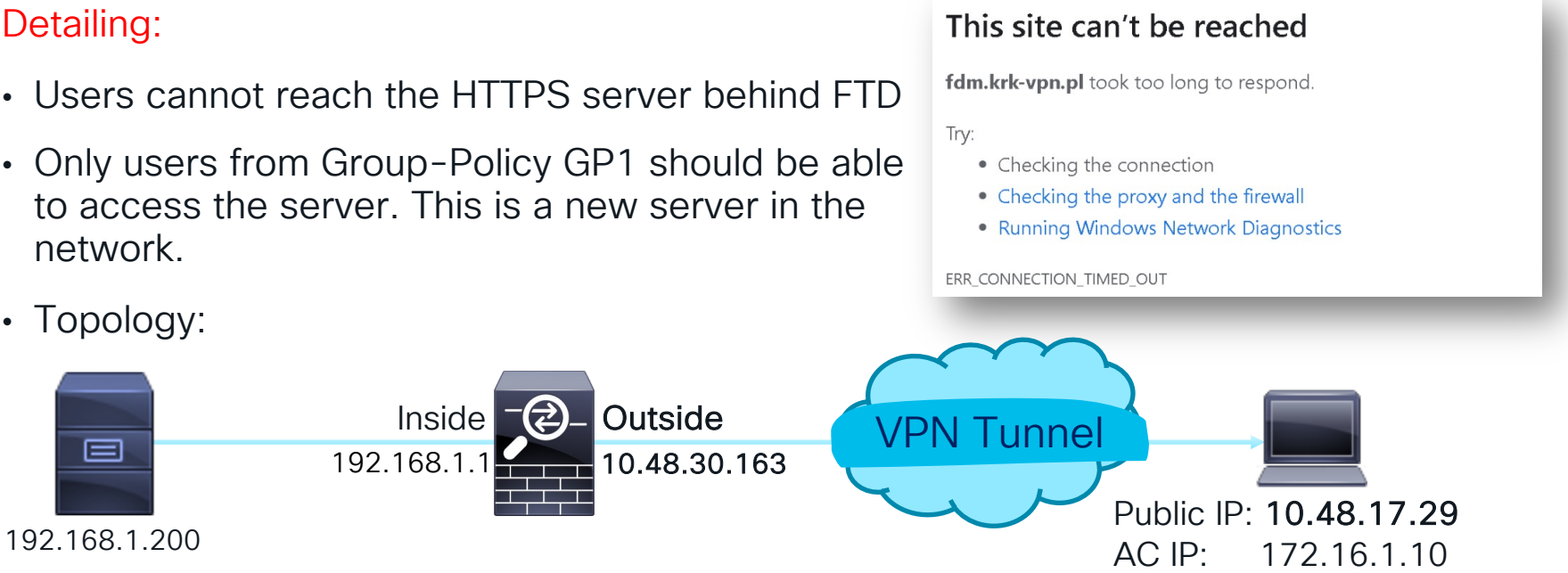
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #7

Reported problem: Users cannot reach the server behind FTD.

Detailing:

- Users cannot reach the HTTPS server behind FTD
- Only users from Group-Policy GP1 should be able to access the server. This is a new server in the network.
- Topology:

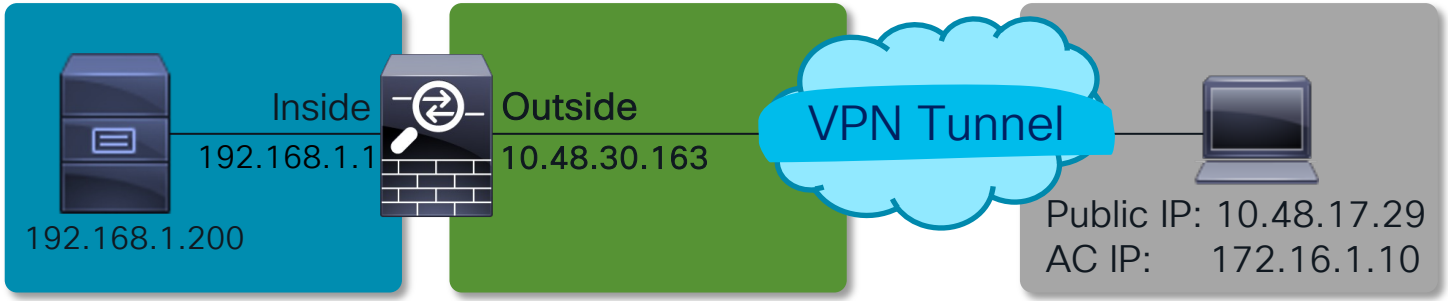


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #7

Triage: Data plane issue.

Action plan: Packet flow needs to be analyzed in multiple places:



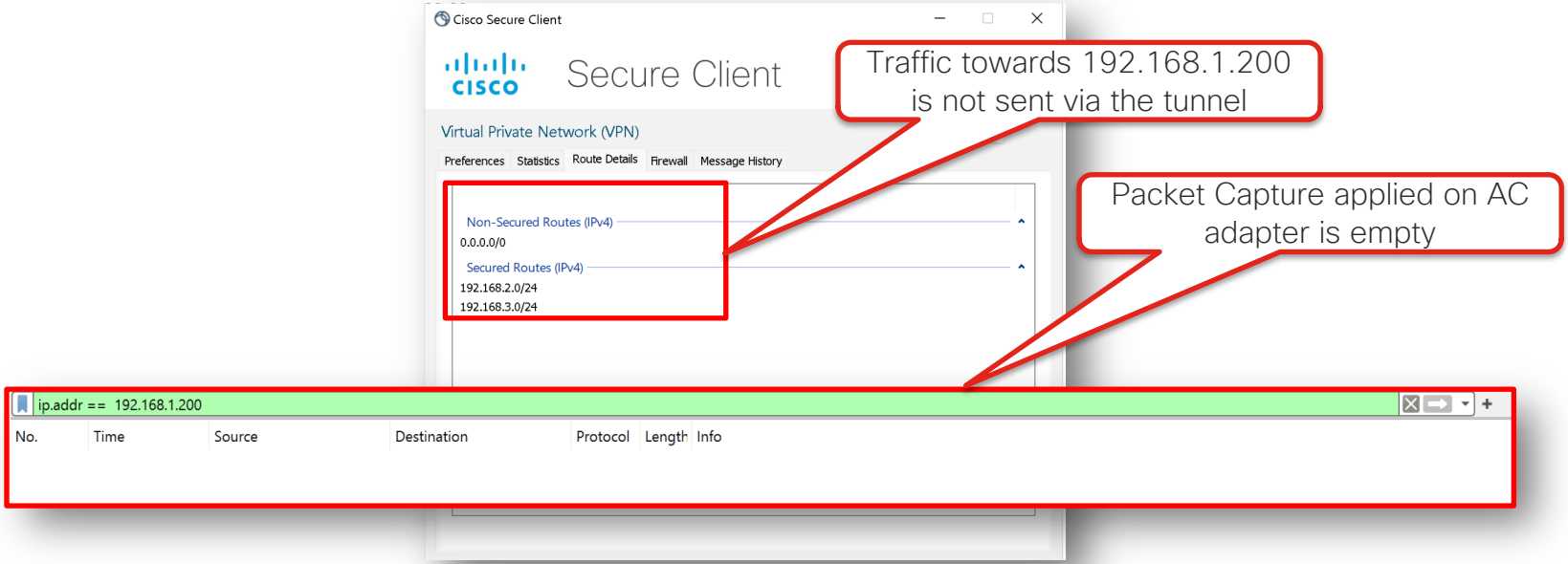
- Host – to confirm if packets are sent via AnyConnect adapter
- FTD Outside network – to check incoming traffic
- FTD Inside network – to check incoming and outgoing traffic

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #7

Investigation:

Step 1: Packet flow on the host:

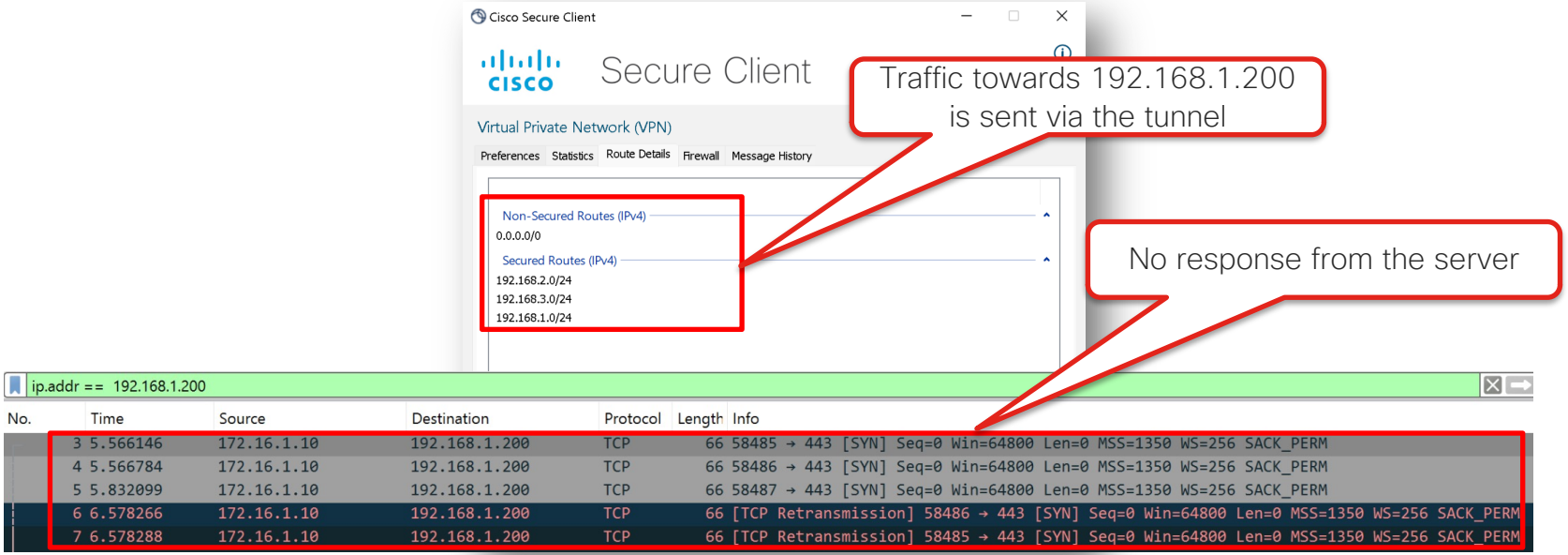


Solution: Split tunnel configuration must be corrected to include the server.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #7

After correcting Split Tunnel configuration, issue is still not resolved but traffic is forwarded via the AnyConnect adapter:



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #7

Only packets from host are seen which is expected

Step 2: Packet Capture on FTD with **include-decrypted** option:

```
 1: 19:01:52.031843       172.16.1.10.58485 > 192.168.1.200.443: S
3197807928:3197807928(0) win 64800 <mss 1350,nop,wscale 8,nop,nop,sackOK>
```

Drop on Access-List Phase

Step 3: Trace for incoming packet:

```
Phase: 5
Type: ACCESS-LIST
Subtype: log
Result: DROP
Elapsed time: 2148 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip any any rule-id 268434432
access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: ACP1 - Default
access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
```

Solution: Traffic from remote clients to the server should be allowed in the Access Control Policy applied on the FTD.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #7

Step 4: After adjusting ACP, traffic is still dropped but on a different phase:

```
Phase: 4
Type: SNORT
Subtype:
Result: DROP
Elapsed time: 26619 ns
Config:
Additional Information:
Snort Verdict: (black-list) black list this flow
```

Traffic is dropped by SNORT

Step 5: Use ‘system support trace’

```
172.16.1.10 58636 -> 192.168.1.200 443 6 AS=0 ID=4 GR=1-1 Verdict: blacklist
172.16.1.10 58636 -> 192.168.1.200 443 6 AS=0 ID=4 GR=1-1 Verdict Reason: reputation,
force_block
172.16.1.10 58637 -> 192.168.1.200 443 6 AS=0 ID=3 GR=1-1 reputation verdict block
from source with list id 1048591
```

Traffic is dropped due to SI blocklist

Solution: Adjust Security Intelligence block list configuration.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #7

Step 6: Collect a fresh packet capture and check traces

```
Result:
input-interface: outside(vrfid:0)
input-status: up
input-line-status: up
output-interface: inside(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 226836 ns
```

Traffic is allowed, no drop on the FTD

Note: If there are no drops on the ASA/FTD, but remote clients are still experiencing the issue, the packet capture can be enabled on the Inside interface and then next hop in the Inside network checked.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Issue #7

Packet Capture on Outside interface

```
firepower# show cap cap1
   1: 19:50:02.648236       172.16.1.10.58737 > 192.168.1.200.443: S
2495261297:2495261297(0) win 64800 <mss 1350,nop,wscale 8,nop,nop,sackOK>
   2: 19:50:02.900084       172.16.1.10.58738 > 192.168.1.200.443: S
190228809:190228809(0) win 64800 <mss 1350,nop,wscale 8,nop,nop,sackOK>
   3: 19:50:03.650158       172.16.1.10.58737 > 192.168.1.200.443: S
2495261297:2495261297(0) win 64800 <mss 1350,nop,wscale 8,nop,nop,sackOK>
```

The same packets seen on Inside interface

```
firepower# show cap cap2
   1: 19:50:02.648678       172.16.1.10.58737 > 192.168.1.200.443: S
2652404264:2652404264(0) win 64800 <mss 1350,nop,wscale 8,nop,nop,sackOK>
   2: 19:50:02.900557       172.16.1.10.58738 > 192.168.1.200.443: S
1164904406:1164904406(0) win 64800 <mss 1350,nop,wscale 8,nop,nop,sackOK>
   3: 19:50:03.650372       172.16.1.10.58737 > 192.168.1.200.443: S
2652404264:2652404264(0) win 64800 <mss 1350,nop,wscale 8,nop,nop,sackOK>
```


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Conclusion

Summary and Take Away...

- Troubleshooting Remote Access issues can be easy!
- The Key is to properly Define and Isolate the problem.
- Use available tools to collect the data: DART bundle, packet capture, syslog messages, debugs and show outputs.
- If collected details are inconclusive – call TAC!
- Upgrade to Secure Client 5.x.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

End of Support Announcement

AnyConnect 4.x

- Software maintenance for 4.x software releases will end on March 31, 2024. No patches or maintenance releases will be provided for AnyConnect 4.x releases after that date.
- Application software support will not be available for the stated software versions beyond March 31, 2027.
- Software maintenance and application software support requires an active term license or active service contract for perpetual licenses. After these dates, all support services for the product are unavailable, and the product becomes obsolete.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Webex App

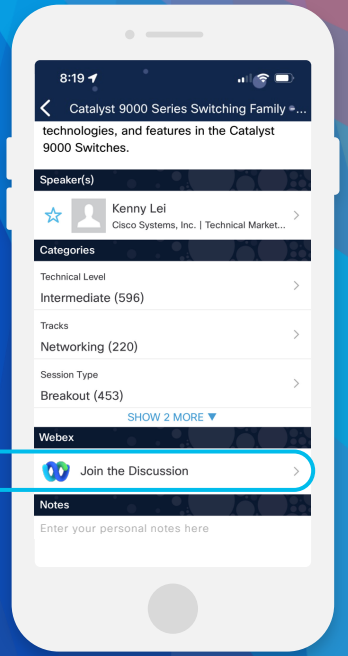
Questions?

Use the Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 23, 2024.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-3935

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fill out your session surveys!



Participants who fill out a minimum of four session surveys and the overall event survey will get a Cisco Live t-shirt (from 11:30 on Thursday, while supplies last)!



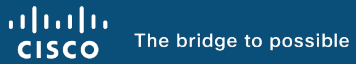
All surveys can be taken in the Cisco Events Mobile App or by logging into the Session Catalog and clicking the 'Participant Resource Center' link at https://www.ciscolive.com/emea/learn/session-catalog.html.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from February 23.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



Thank you




cisco Live!
Let's go