FALCO

TLS Inbound Inspection

Like outbound-decrypt, but better.

Why do we need decryption?

What the firewall sees *without* decryption:

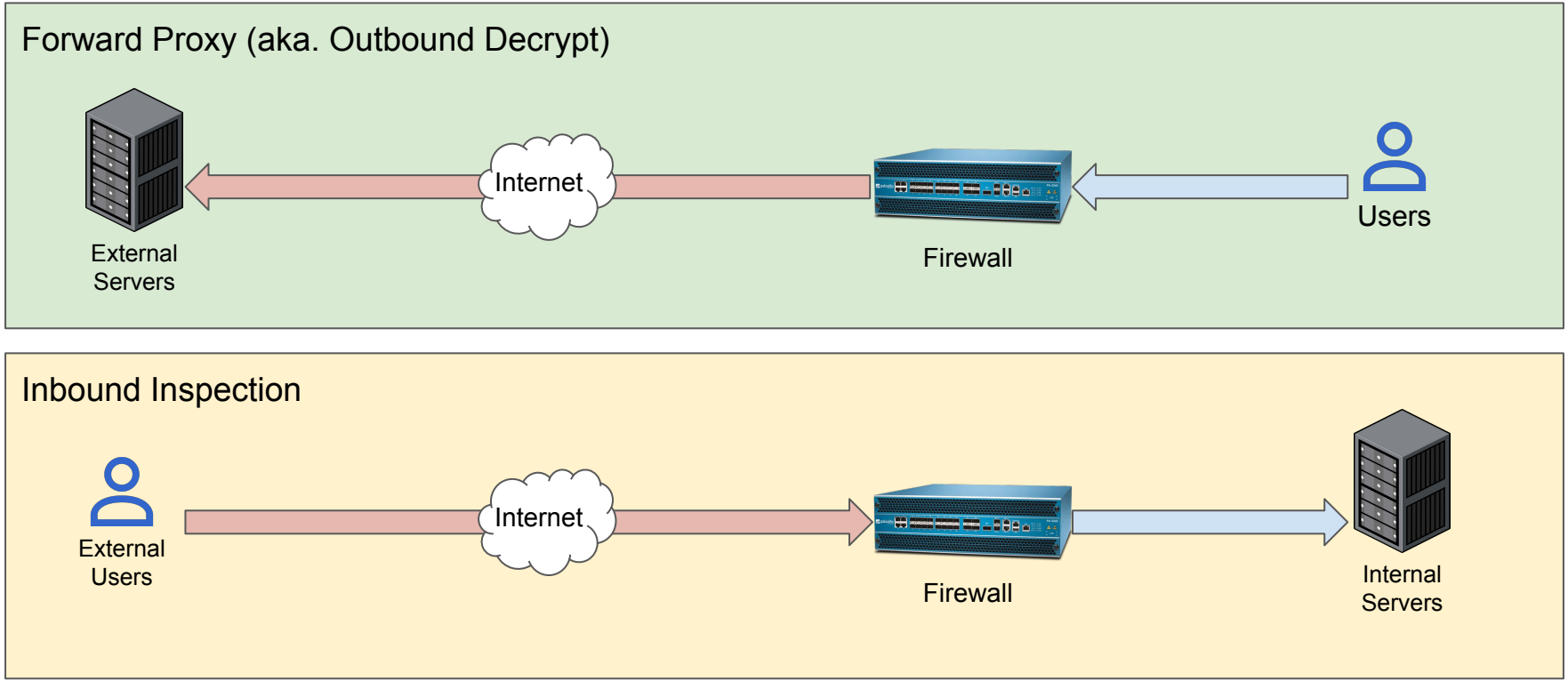
.....uJ...l.>k.;..;....g.....1..... ...k.}..>l.h.>..o0...|.....~
..."....+./.....,.0.
. ...../.5.....example.com.....
.....#.....h2.http/1.1.....".
.....3.k.i...
X.-DS..!c..>...d.....fG.9..}.....A...Q... }.[G.....Nr}r....6S!.y.....5.!,..'....o..E.S.Zte\../....+.....
.....-.....@.....x..{.t....'.{.....*..bsj.S
...k.}..>l.h.>..o0...|.....~
.....O.+.....3.E...A..r....0{.(.....!.@..L.....0:.....-.....~....Loep.\."..... .<k.T.7v...u....Mm.H|.
tal.lXB.....a_.M[.K...!...*...9.....5..U.....^/.W.b :.r....s..].n.@.....d...5.w....
.....5...dx..0..O.Lm.....w.yo.....Ep.....c1EL...2.q.f.3.O..t.=C.Y..k.n...fw..r.?9.=T..>.....O~...d,QB.m.kl.a.Q.
...YUM.y.n....4=..[.g...h....}.....<..6.&7...".B.T.;.L.i.E.<r.""../.Snx..K..
.rj..zBX.sE.u.....{~.A.Z@L.Y.
..{...`..Ynh..*;;!.....&.2.`T.V2e.,B....J...^.!"v.teC..W.'..k.... .
..X.L..~NUw.....S..Hc"|....7....9._...7A.@.+....F....u..d...6.Q...z..R.5.C.....z_..*.D...F.....*Ct9J.....by...,...jh.|.&./E.GfOY]...;-...(.kE.a.....
..s...?....&.d.).....C.....e.#3f.a...:D.....U...1...Ut..).?....P..V\".....
....<...`.r3[...._,R.

What the firewall sees *with* decryption:

```
GET /classes/details?id=CS101; DROP TABLE STUDENTS; HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

HTTP/1.1 200 OK
Content-Encoding: gzip
Accept-Ranges: bytes
Age: 460608
Cache-Control: max-age=604800
Content-Type: text/html; charset=UTF-8
Date: Mon, 21 Mar 2022 23:54:11 GMT
```

Forward Proxy vs. Inbound Inspection

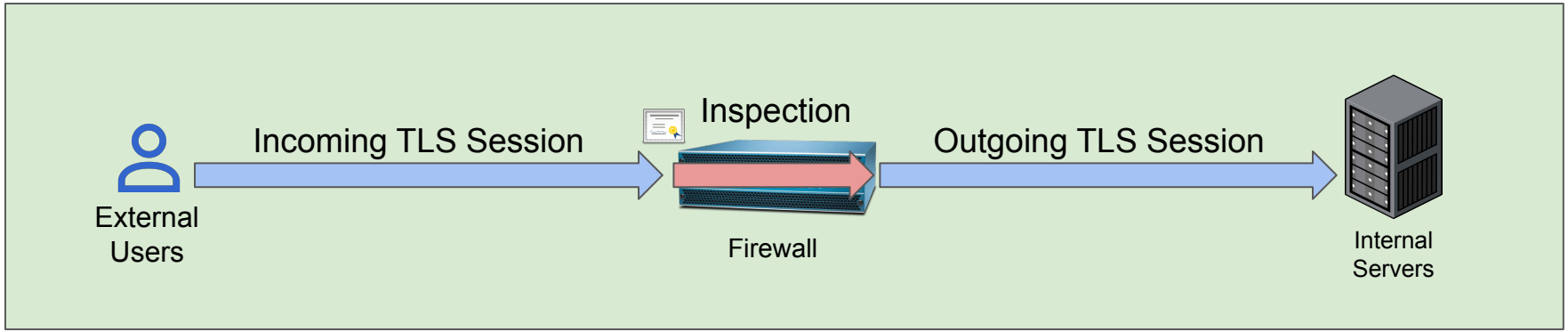


Outbound vs. Inbound

- CA cert must be installed on all devices
- Outbound decrypt requires constant tuning
- Not all site traffic can be decrypted
- Can’t decrypt devices you don’t control
- Protects user from themselves

- Certs installed on the firewall
- Configured once, updated occasionally
- All services you control can be decrypted
- Only need control of the server side
- Protects servers from outside attackers

How it works: Low-Level

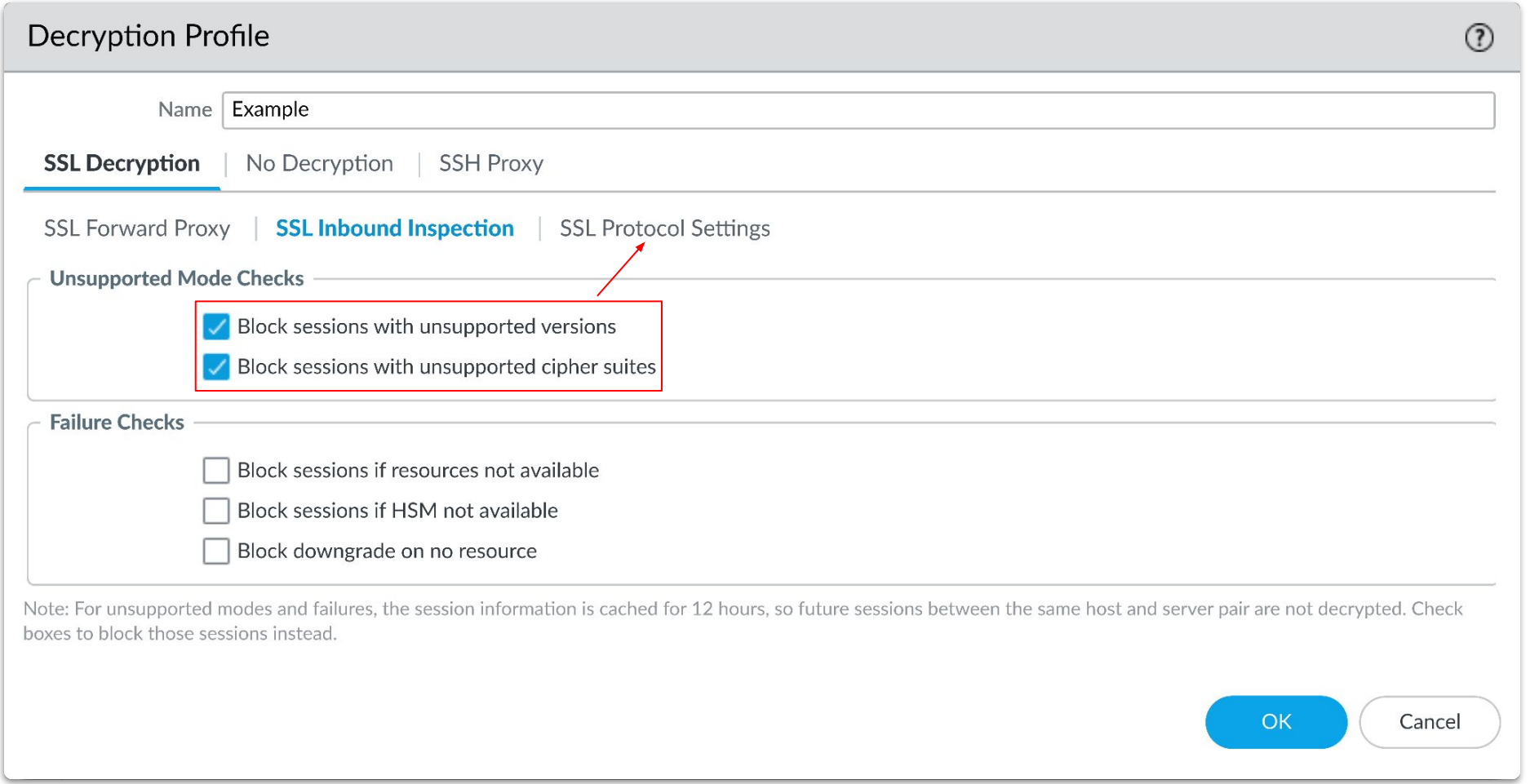


Inbound Inspection Requirements

- Valid public certificates for the servers you want to intercept
- An understanding of the TLS versions & ciphers currently in-use
- No client cert based authentication

Inbound Inspection Project Plan

1. Ensure that all decrypting firewalls are running PAN-OS ≥ 10.0.0
2. Get a list of all the services you want to decrypt
3. Identify any need for specific TLS versions or ciphers
4. Gather certificates for all services (or a wildcard if possible)
5. Import all certificates into the firewall
6. Create a decryption profile
7. Create decryption rules to decrypt inbound connections to those services
8. Validate that applications work as expected


Decryption Profile
Name
Example
SSL Decryption
No Decryption
SSH Proxy
SSL Forward Proxy
SSL Inbound Inspection
SSL Protocol Settings
Unsupported Mode Checks
Block sessions with unsupported versions
Block sessions with unsupported cipher suites
Failure Checks
Block sessions if resources not available
Block sessions if HSM not available
Block downgrade on no resource
Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.
OK
Cancel

Aside: TLS Details

- In TLS a client and server must agree on details of three algorithms
  - Key Exchange
  - Encryption
  - Authentication
- **Key exchange** allows the peers to determine a shared secret key
- **Encryption** obscures the contents of the stream to prevent eavesdropping
- **Authentication** makes sure that an attacker hasn't tampered with the data
- There are lots of options for each
- Many options are insecure
- Future TLS versions are removing options to ensure security

Key exchange/agreement and authentication

Algorithm	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3	Status
RSA	Yes	Yes	Yes	Yes	Yes	No	
DH-RSA	No	Yes	Yes	Yes	Yes	No	
DHE-RSA (forward secrecy)	No	Yes	Yes	Yes	Yes	Yes	
ECDH-RSA	No	No	Yes	Yes	Yes	No	
ECDHE-RSA (forward secrecy)	No	No	Yes	Yes	Yes	Yes	
DH-DSS	No	Yes	Yes	Yes	Yes	No	
DHE-DSS (forward secrecy)	No	Yes	Yes	Yes	Yes	No[55]	
ECDH-ECDSA	No	No	Yes	Yes	Yes	No	
ECDHE-ECDSA (forward secrecy)	No	No	Yes	Yes	Yes	Yes	
ECDH-EdDSA	No	No	Yes	Yes	Yes	No	
ECDHE-EdDSA (forward secrecy)[56]	No	No	Yes	Yes	Yes	Yes	Defined for TLS 1.2 in RFCs
PSK	No	No	Yes	Yes	Yes		
PSK-RSA	No	No	Yes	Yes	Yes		
DHE-PSK (forward secrecy)	No	No	Yes	Yes	Yes	Yes	
ECDHE-PSK (forward secrecy)	No	No	Yes	Yes	Yes	Yes	
SRP	No	No	Yes	Yes	Yes		
SRP-DSS	No	No	Yes	Yes	Yes		
SRP-RSA	No	No	Yes	Yes	Yes		
Kerberos	No	No	Yes	Yes	Yes		
DH-ANON (insecure)	No	Yes	Yes	Yes	Yes		
ECDH-ANON (insecure)	No	No	Yes	Yes	Yes		
GOST R 34.10-94 / 34.10-2001[57]	No	No	Yes	Yes	Yes		Proposed in RFC drafts

Source: https://en.wikipedia.org/wiki/Transport_Layer_Security#Key_exchange_or_key_agreement

Cipher			Cipher security against publicly known feasible attacks: Protocol version					
Type	Algorithm	Nominal strength (bits)	SSL 2.0	SSL 3.0 [n 1][n 2][n 3][n 4]	TLS 1.0 [n 1][n 3]	TLS 1.1 [n 1]	TLS 1.2 [n 1]	TLS 1.3
Block cipher with mode of operation	AES GCM[58][n 5]	256, 128	N/A	N/A	N/A	N/A	Secure	Secure
	AES CCM[59][n 5]		N/A	N/A	N/A	N/A	Secure	Secure
	AES CBC[n 6]		N/A	Insecure	Depends on mitigations	Depends on mitigations	Depends on mitigations	N/A
	Camellia GCM[60][n 5]	256, 128	N/A	N/A	N/A	N/A	Secure	N/A
	Camellia CBC[61][n 6]		N/A	Insecure	Depends on mitigations	Depends on mitigations	Depends on mitigations	N/A
	ARIA GCM[62][n 5]	256, 128	N/A	N/A	N/A	N/A	Secure	N/A
	ARIA CBC[62][n 6]		N/A	N/A	Depends on mitigations	Depends on mitigations	Depends on mitigations	N/A
	SEED CBC[63][n 6]	128	N/A	Insecure	Depends on mitigations	Depends on mitigations	Depends on mitigations	N/A
	3DES EDE CBC[n 6][n 7]	112[n 8]	Insecure	Insecure	Insecure	Insecure	Insecure	N/A
	GOST 28147-89 CNT[57][n 7]	256	N/A	N/A	Insecure	Insecure	Insecure	N/A
	IDEA CBC[n 6][n 7][n 9]	128	Insecure	Insecure	Insecure	Insecure	N/A	N/A
	DES CBC[n 6][n 7][n 9]	56	Insecure	Insecure	Insecure	Insecure	N/A	N/A
		40[n 10]	Insecure	Insecure	Insecure	N/A	N/A	N/A
	RC2 CBC[n 6][n 7]	40[n 10]	Insecure	Insecure	Insecure	N/A	N/A	N/A
Stream cipher	ChaCha20-Poly1305[68][n 5]	256	N/A	N/A	N/A	N/A	Secure	Secure
	RC4[n 11]	128	Insecure	Insecure	Insecure	Insecure	Insecure	N/A
		40[n 10]	Insecure	Insecure	Insecure	N/A	N/A	N/A
None	Null[n 12]	–	Insecure	Insecure	Insecure	Insecure	Insecure	N/A

Source: https://en.wikipedia.org/wiki/Transport_Layer_Security#Cipher

Data integrity

Algorithm	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3	Status
HMAC-MD5	Yes	Yes	Yes	Yes	Yes	No	Defined for TLS 1.2 in RFCs
HMAC-SHA1	No	Yes	Yes	Yes	Yes	No	
HMAC-SHA256/384	No	No	No	No	Yes	No	
AEAD	No	No	No	No	Yes	Yes	
GOST 28147-89 IMIT[57]	No	No	Yes	Yes	Yes		Proposed in RFC drafts
GOST R 34.11-94[57]	No	No	Yes	Yes	Yes		

Source: https://en.wikipedia.org/wiki/Transport_Layer_Security#Data_integrity

TLS 1.3 - OTHER

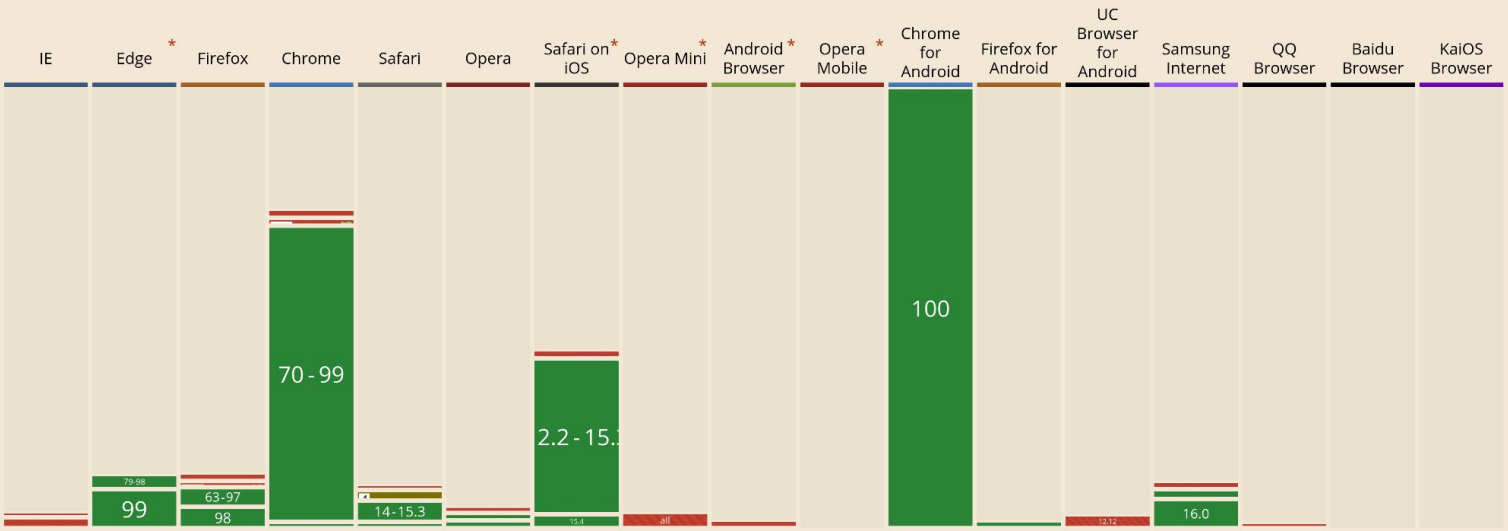
Version 1.3 (the latest one) of the Transport Layer Security (TLS) protocol. Removes weaker elliptic curves and hash functions.

Usage: Global

% of all users ?

90.39% + 0.58% = 90.97%

Current aligned | Usage relative | Date relative | Filtered | All



Notes | Test on a real browser | Known issues (0) | Resources (5) | Feedback

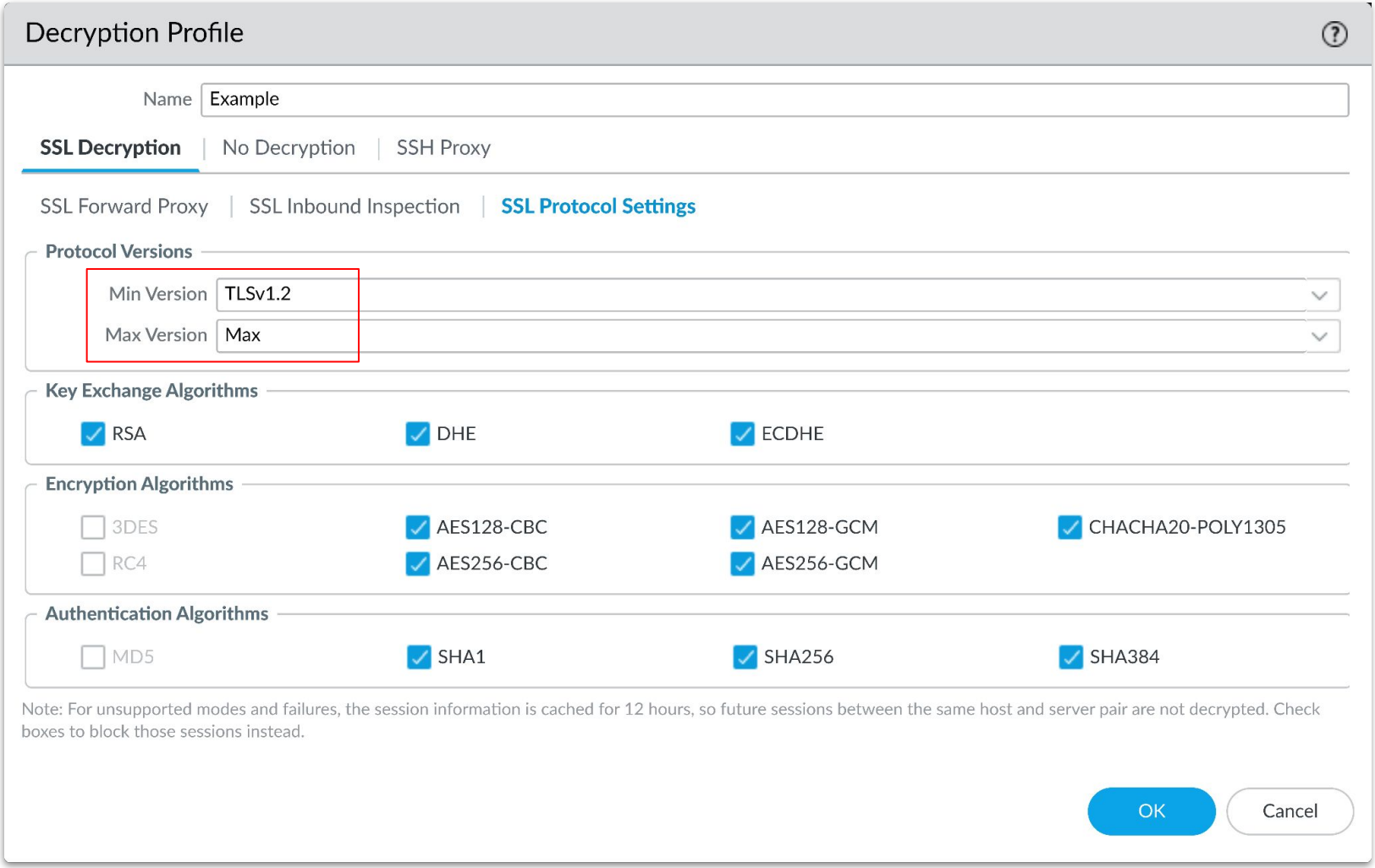
1 Supports a draft of the TLS 1.3 specification, not the final version.

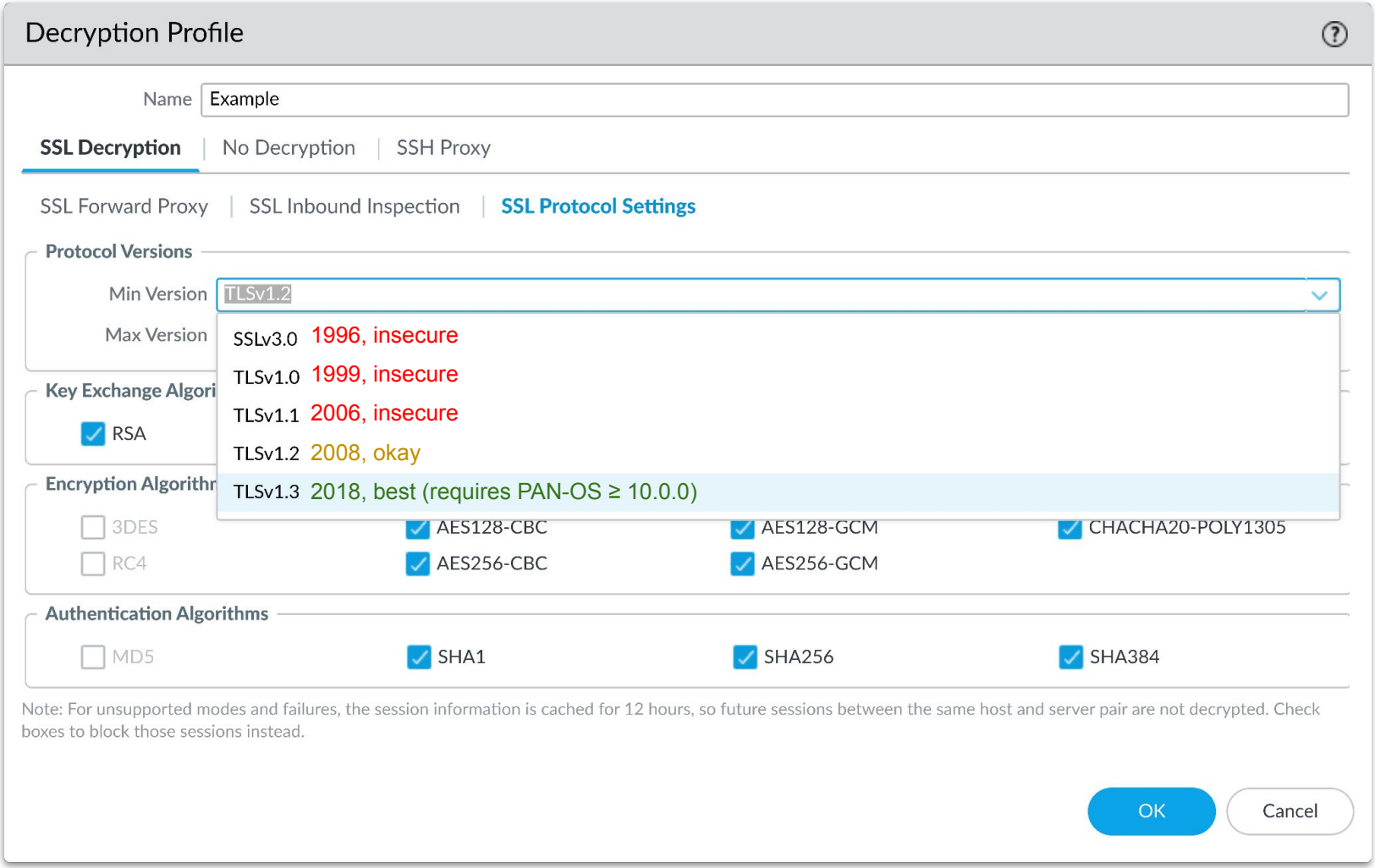
2 Can be enabled in Firefox by setting the `security.tls.version.max` pref to "4" in `about:config`.

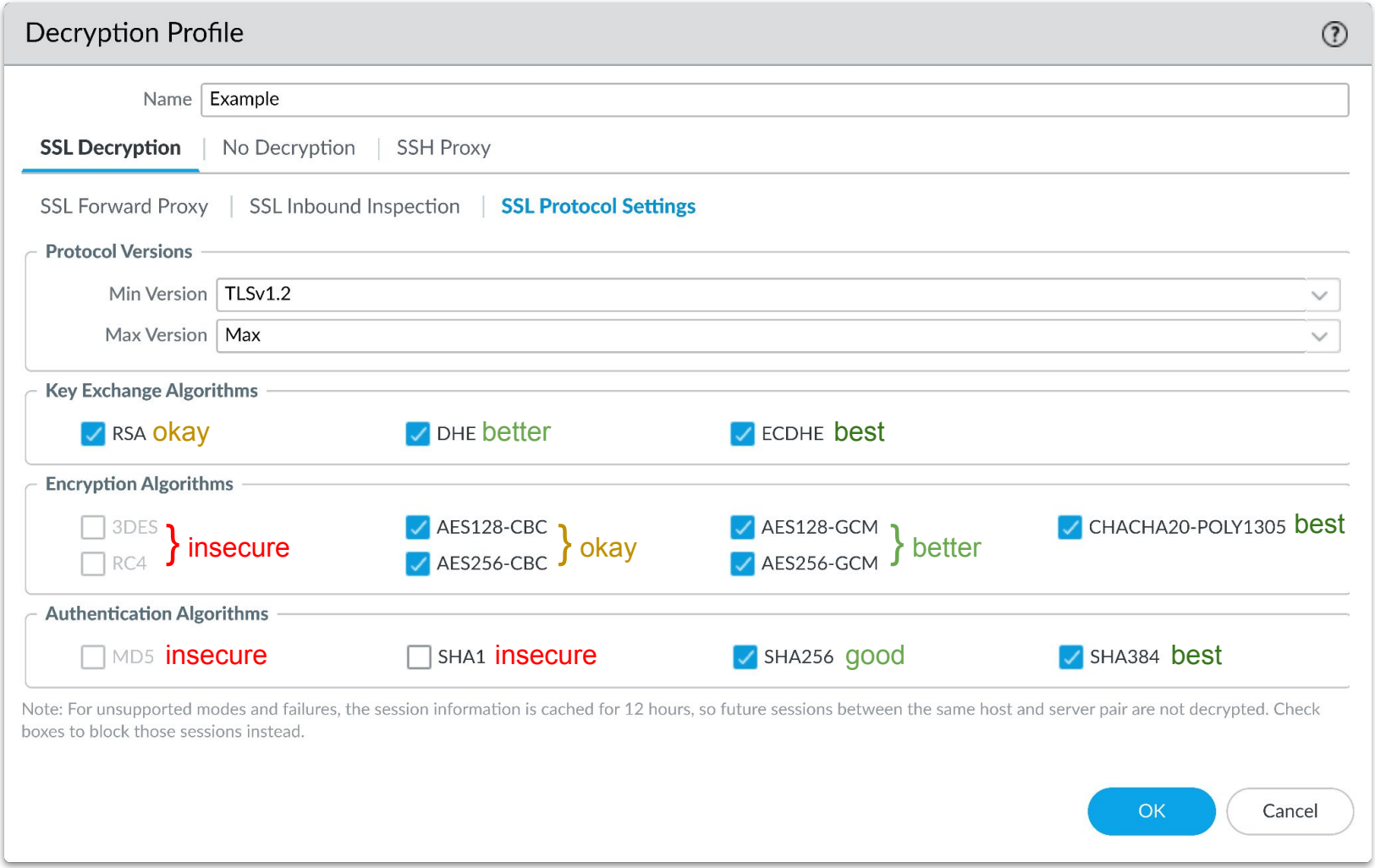
3 Can be enabled in Chrome and Opera via the `#tls13-variant` flag in `chrome://flags` or `opera://flags`.

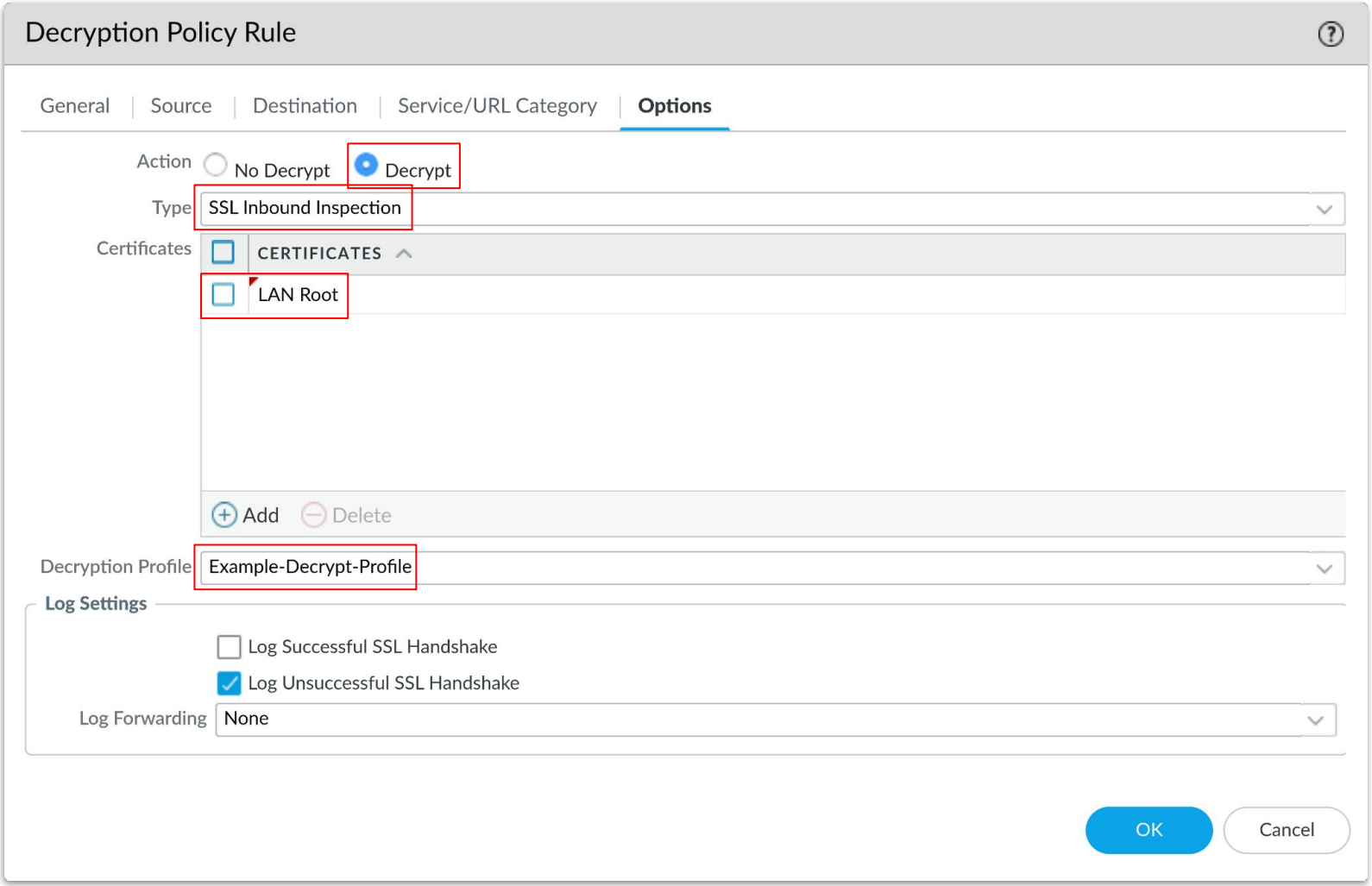
4 Partial support in Safari refers to being limited to macOS 10.14 Mojave and later.

Source: https://caniuse.com/tls1-3


Decryption Profile
Name
Example
SSL Decryption
No Decryption
SSH Proxy
SSL Forward Proxy
SSL Inbound Inspection
SSL Protocol Settings
Protocol Versions
Min Version
TLSv1.2
Max Version
Max
Key Exchange Algorithms
RSA
DHE
ECDHE
Encryption Algorithms
3DES
RC4
AES128-CBC
AES256-CBC
AES128-GCM
AES256-GCM
CHACHA20-POLY1305
Authentication Algorithms
MD5
SHA1
SHA256
SHA384
Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.
OK
Cancel


Decryption Profile
Name
Example
SSL Decryption
No Decryption
SSH Proxy
SSL Forward Proxy
SSL Inbound Inspection
SSL Protocol Settings
Protocol Versions
Min Version
TLSv1.2
Max Version
SSLv3.0 1996, insecure
TLSv1.0 1999, insecure
TLSv1.1 2006, insecure
TLSv1.2 2008, okay
TLSv1.3 2018, best (requires PAN-OS ≥ 10.0.0)
Key Exchange Algori
RSA
Encryption Algorithr
3DES
RC4
AES128-CBC
AES256-CBC
AES128-GCM
AES256-GCM
CHACHA20-POLY1305
Authentication Algorithms
MD5
SHA1
SHA256
SHA384
Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.
OK
Cancel


Decryption Profile
Name
Example
SSL Decryption
No Decryption
SSH Proxy
SSL Forward Proxy
SSL Inbound Inspection
SSL Protocol Settings
Protocol Versions
Min Version
TLSv1.2
Max Version
Max
Key Exchange Algorithms
RSA okay
DHE better
ECDHE best
Encryption Algorithms
3DES
RC4
insecure
AES128-CBC
AES256-CBC
okay
AES128-GCM
AES256-GCM
better
CHACHA20-POLY1305 best
Authentication Algorithms
MD5 insecure
SHA1 insecure
SHA256 good
SHA384 best
Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.
OK
Cancel


Decryption Policy Rule
General
Source
Destination
Service/URL Category
Options
Action
No Decrypt
Decrypt
Type
SSL Inbound Inspection
Certificates
CERTIFICATES
LAN Root
Add
Delete
Decryption Profile
Example-Decrypt-Profile
Log Settings
Log Successful SSL Handshake
Log Unsuccessful SSL Handshake
Log Forwarding
None
OK
Cancel

GENERATE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	DECRYPTED	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON
03/31 17:13:57	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	websocket	allow	Allow Admins to Inside	tcp-fin
03/31 16:51:45	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	git-base	allow	Allow Admins to Inside	aged-out
03/31 16:51:34	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:51:33	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:46:28	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:41:54	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	websocket	allow	Allow Admins to Inside	tcp-fin
03/31 16:41:23	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:36:20	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:31:17	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:26:45	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	8443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:26:45	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	8443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:26:13	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:21:19	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	git-base	allow	Allow Admins to Inside	aged-out
03/31 16:21:08	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:21:07	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:16:03	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out
03/31 16:10:59	end	vpn	inside	172.21.2.7	ds\zsum	10.1.131.35	yes	443	github-base	allow	Allow Admins to Inside	aged-out

Detailed Log View

General

Session ID	71357
Action	allow
Action Source	from-policy
Host ID	
Application	websocket
Rule	Allow Admins to Inside
Rule UUID	17a9c58f-c013-43f0-b7b6-1d1951bbd124
Session End Reason	tcp-fin
Category	computer-and-internet-info
Device SN	011901033264
IP Protocol	tcp
Log Action	lf_standard
Generated Time	2022/03/31 17:13:57
Start Time	2022/03/31 16:41:37
Receive Time	2022/03/31 17:14:07
Elapsed Time(sec)	1920
Tunnel Type	N/A

Source

Source User	ds\zsum
Source	172.21.2.7
Source DAG	
Country	172.16.0.0-172.31.255.255
Port	1912
Zone	vpn
Interface	tunnel.1
X-Forwarded-For IP	0.0.0.0

Destination

Destination User	
Destination	10.1.131.35
Destination DAG	
Country	10.0.0.0-10.255.255.255
Port	443
Zone	inside
Interface	ae1.911

Details

Type	end
Bytes	24528
Bytes Received	12904
Bytes Sent	11624
Repeat Count	1
Packets	186
Packets Received	80
Packets Sent	106
Source UUID	
Destination UUID	

Flags

- Captive Portal ☐
- Proxy Transaction ☐
- Decrypted ☑
- Packet Capture ☐
- Client to Server ☐
- Server to Client ☐
- Symmetric Return ☐
- Mirrored ☐
- Tunnel Inspected ☐
- MPTCP Options ☐
- Recon excluded ☐

PCAP	RECEIVE TIME	TYPE	APPLICATION	ACTION	RULE	RULE UUID	BYTES	SEVERITY	CATEGORY	URL CATEGORY LIST	VERDICT	URL	FILE NAME
	2022/03/31 17:14:07	end	websocket	allow	Allow Admins to Inside	17a9c58f-c0...	24528		computer-and-internet-info				

Close

Troubleshooting

- Very similar to outbound decrypt
- Use **Monitor** → **Logs** → **Decryption** (only in PAN-OS ≥ 10.0.0)
- Look for the **Error** and **Error Index** columns
- Most likely an incompatibility with the TLS version/cipher
- Use packet captures & hardware counters
  - `show counter global filter packet-filter yes delta yes`

Q & A

Thanks for attending!

Questions: support@digitalscepter.com

Contact: coleman@digitalscepter.com

Complaints: zach@digitalscepter.com