BIG-IP TMOS 12.x Update

Jason Smith – Sr Technical Trainer EMEA

Why Migrate From Older Releases?

Software Quality

Long-term stability and supportability

Business Transformation

Industry-leading flexibility and support for Cloud

Security Focus

Protect against sophisticated attacks

Hardware

New Hardware

BIG-IP 12250V

- Best price/performance for SSL in it’s class
- Support for 24 vCMP guests

VIPRION B4450

- First ADC to support 100G QSFP28 form factor
- Build 1Tbps+ platforms

ADC and TMOS

ADC/TMOS 12.x Highlights

iApps & iRules LX

External Crypto Offload

SSL Mirroring

iAppsLX vs "Traditional" iApps

Traditional iApps

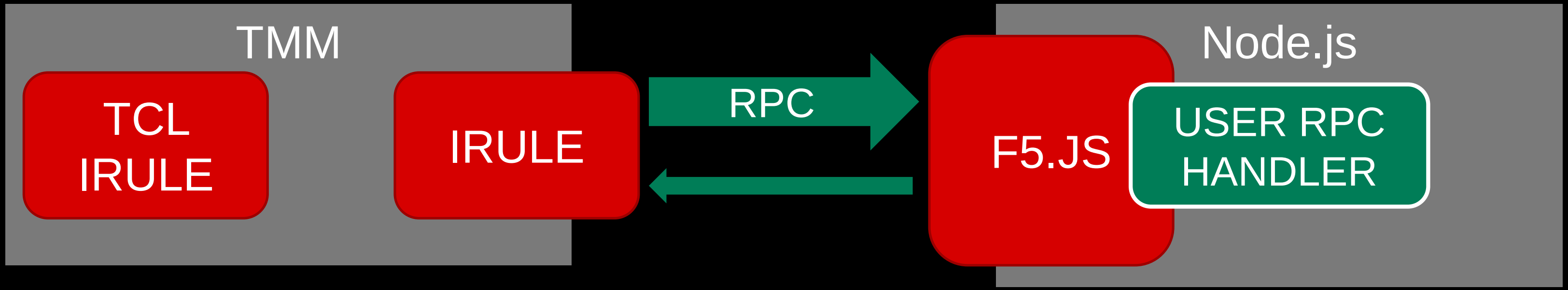
- Based on TCL
- Runs TMSH commands to change config
- BIG-IP only
- No application-level statistics

iAppsLX

- Based on JavaScript
- Performs REST API calls to change config
- Multi-platform support
- Designed for stats and health roll-up

iRules Language Extensions (LX)

- iRules TCL is here to stay, and remains very well integrated
- iRules LX is out-of-band, will provide access to more languages and libraries
- First implementation is with Node.js



SSL External Crypto Offload

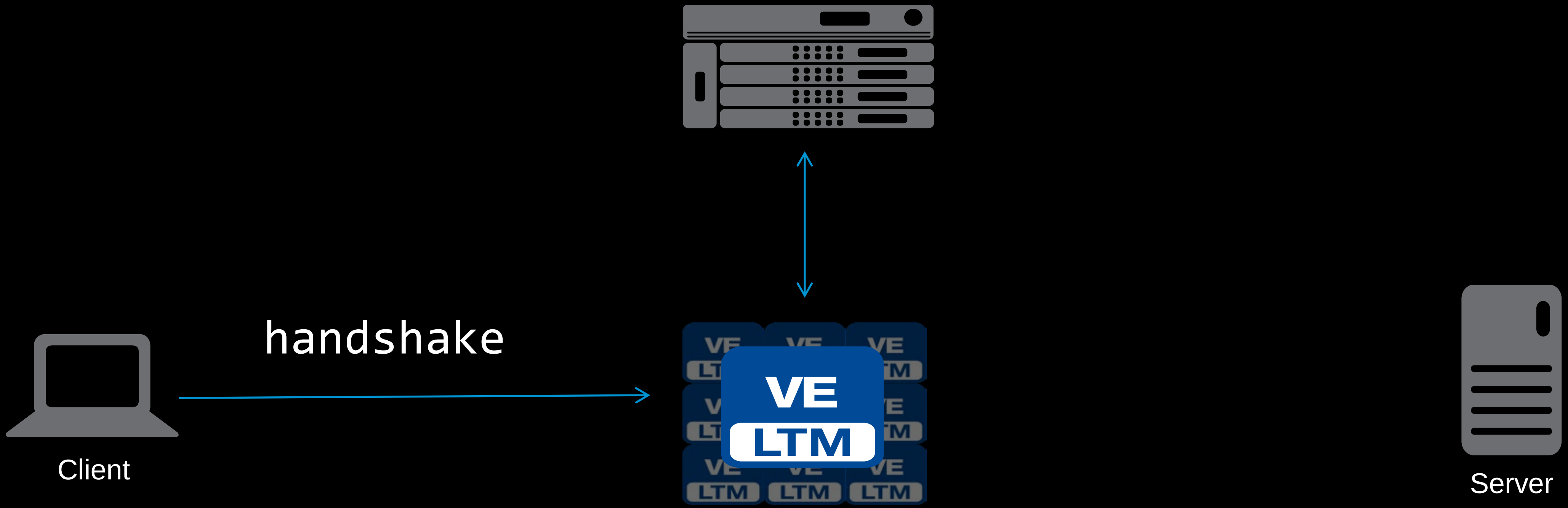
Problem:

Customers deploy low-performing SSL platforms (VE) but want to maximise their SSL performance and license

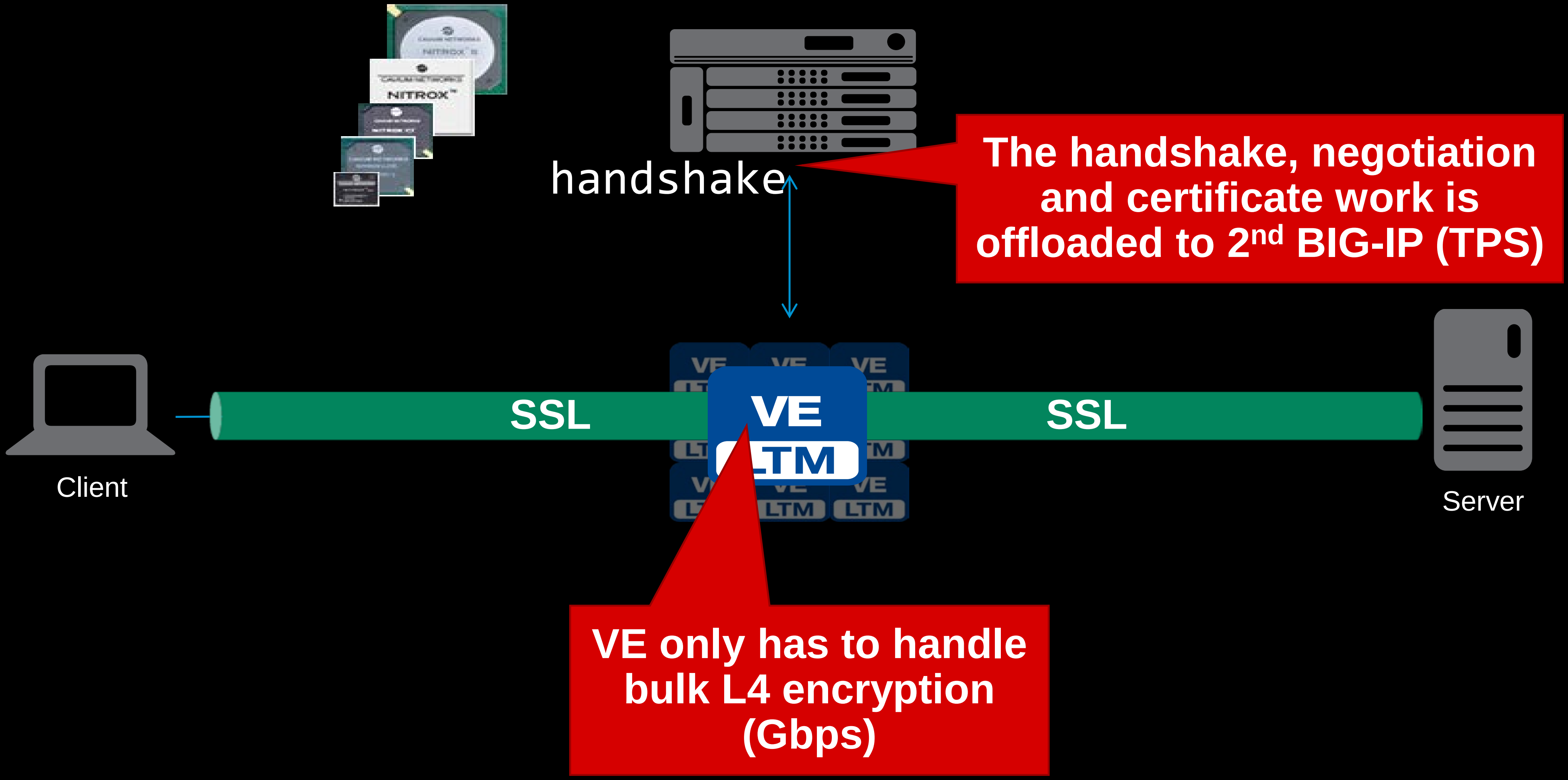
Performance example

Platform	License TPS	Actual TPS
Quad Core 2Ghz x86 VE	2000	**700**
VE Offload to 10200V	75000	**5700**

SSL Crypto Offload



SSL Crypto Offload



The handshake, negotiation and certificate work is offloaded to 2nd BIG-IP (TPS)

VE only has to handle bulk L4 encryption (Gbps)

SSL Connection & Session Mirroring

- Setting up of the SSL connection is the most expensive part of the process
- Anything we can do to prevent re-doing this (in a failure scenario) is valuable
- Useful for long-lived SSL connections:
  - ATM machines
  - Streaming video over HTTPS
  - Online gaming

BIG-IP ADC/TMOS Summary

Flexibility

Incredible flexibility for unique customer environments

Security

Leading platform for managing SSL with unmatched performance

Access Policy Manager (APM)

APM 12.x Highlights

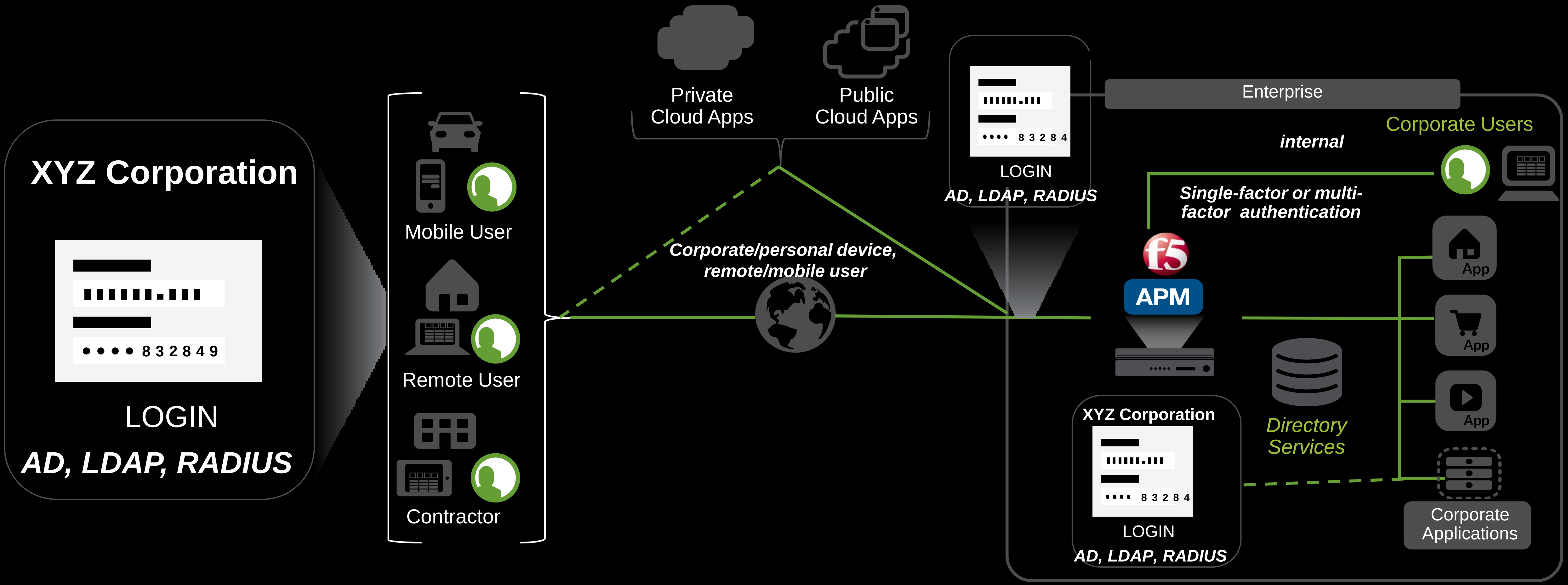
Step-Up Authentication

Best in class VDI Support

MDM Integration

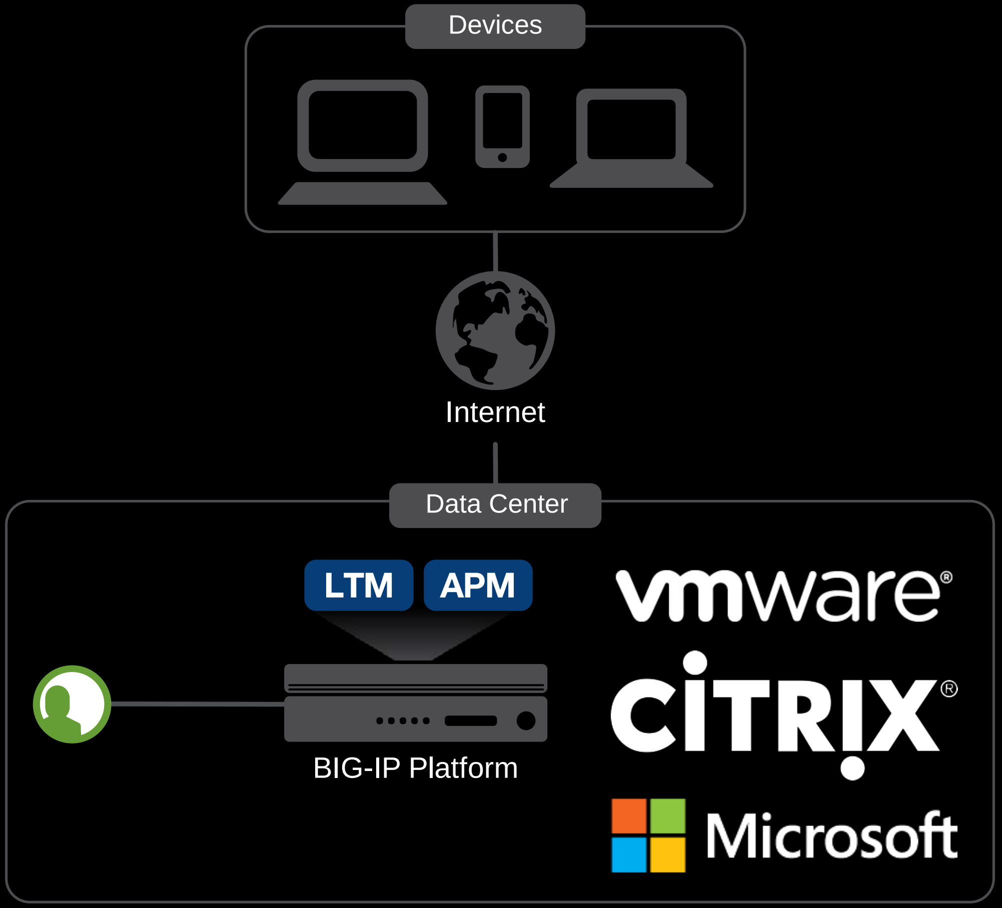
Step-up Authentication (Preview)

Anonymous access to and re-validation of AD, LDAP, or RADIUS authentication per request within an access session, for accessing additional, sensitive web URIs, or to extend a session

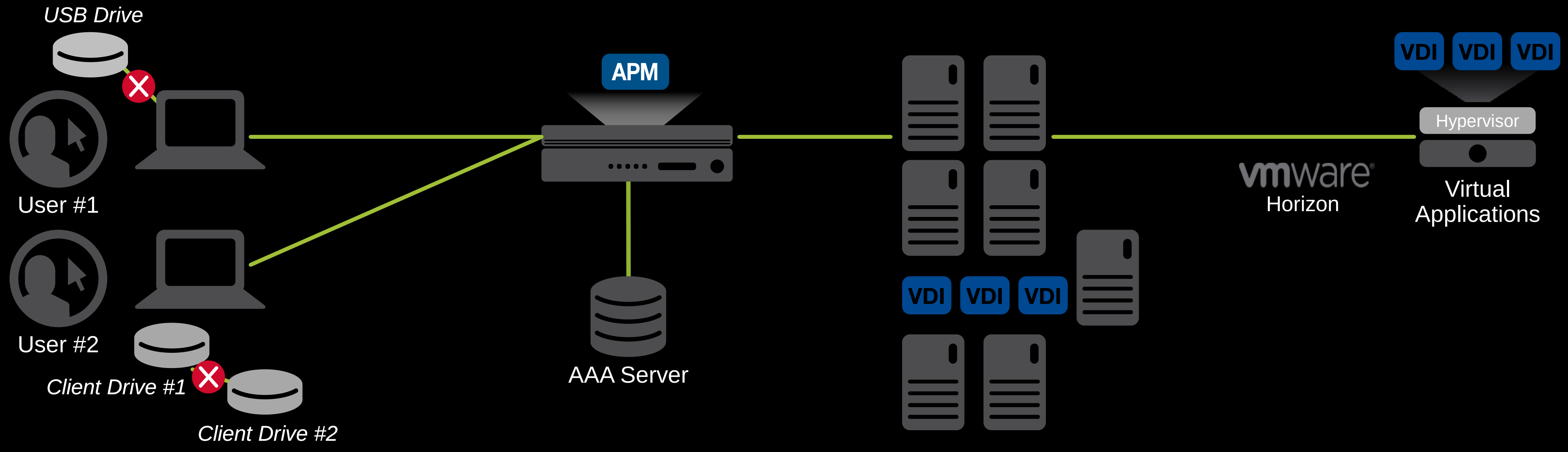


Best in Class VDI Support

- Native, full-proxy support for all major vendors
- Simplify your VDI deployment and reduce device sprawl
- Fast implementation with iApps



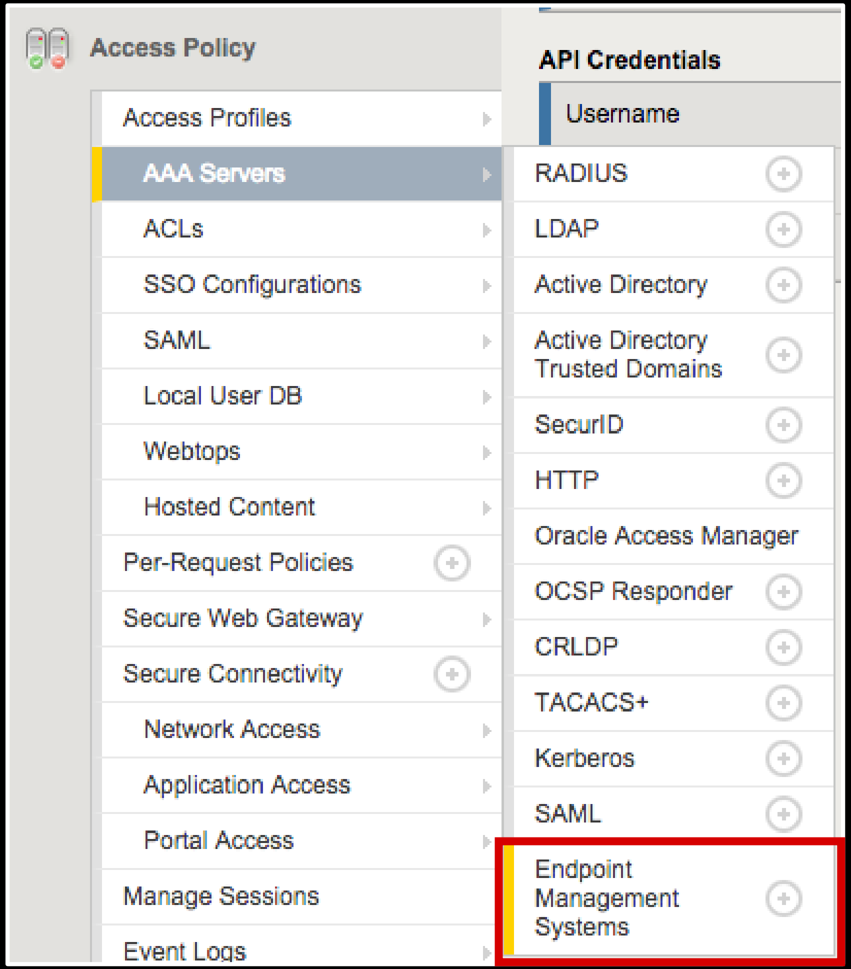
Support and Control USB Redirection and Client Drive Mapping for VMware Horizon

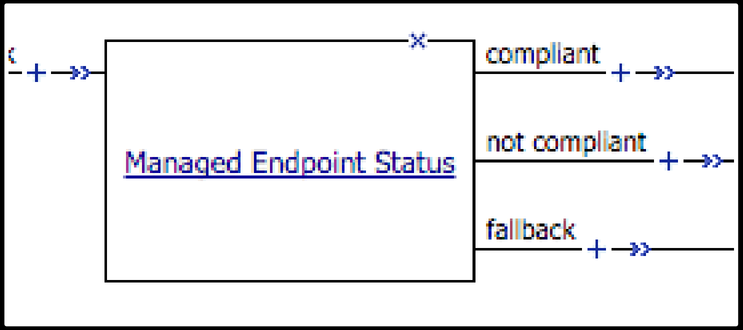


- BIG-IP APM empowers enterprises via identity-aware, context-based policies to control the use of USB devices by VMware Horizon users and their devices
- Identity-aware, context-based control over client drive redirection
- APM mitigates and protects against data loss for managed accounts and devices

New Endpoint Management Querying agent for MDM

- Ability to tightly integrate APM with endpoint management systems
- 12.0 brings support for Airwatch and Fiberlink. More will come later
- Implemented as a AAA object and a VPE action





New MDM session variables

These will populate on successful execution of the agent

MDM VALUE	SESSION VARIABLE
Internal MDM ID	session.mdm.device.
UDID	session.mdm.device.udid
Mac Address	session.mdm.device.mac
Serial Number	session.mdm.device.serial
IMEI	session.mdm.device.imei
ActiveSync ID	session.mdm.device.activesyncid
is_enrolled	session.mdm.device.enrolled
is_compliant	session.mdm.device.compliant
last_compliance_check	session.mdm.device.lastcompliancecheck
Username	session.mdm.device.username

BIG-IP APM Summary

Simplifies

Improves performance and usability, while simplifying administration

Secures

Enhances application and virtualized apps and desktop security

Protects

Expands data loss prevention and guards against web-based attacks

Advanced Firewall Manager (AFM)

AFM 12.x Highlights

Advanced DoS Protection

SSH Proxy

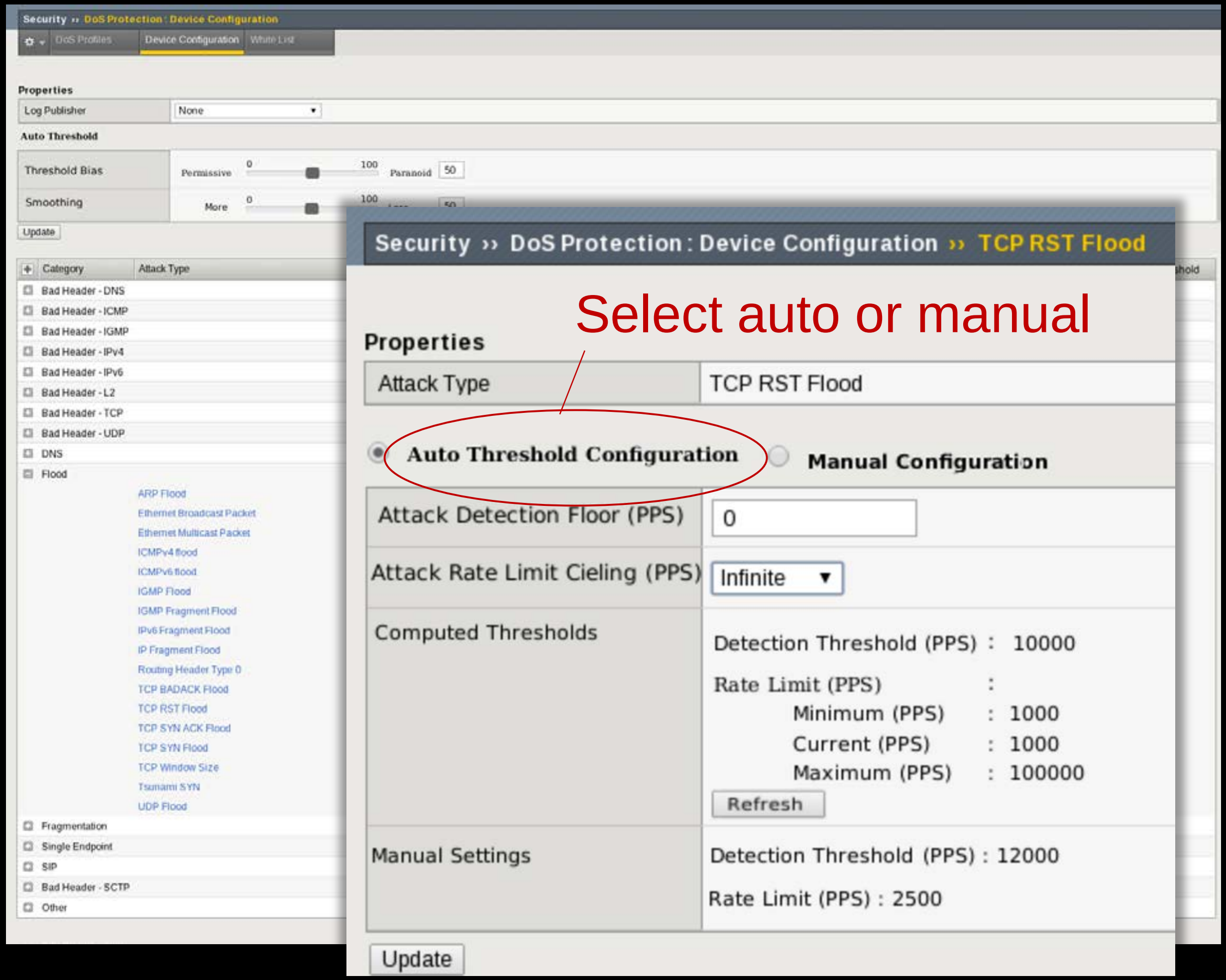
Firewall NAT

Advanced DoS Protection

- Layered DoS mitigation – **Device** and **Application** protection
- **Hardware** offload for 100+ DoS vectors
- Endpoint aware Sweep/Flood protection
  - Sweep – single **Client IP** to multiple endpoints
  - Flood – many devices attacking single **Destination IP**
- **Self-tuning** DoS thresholds

Greater effectiveness with self-tuning DDoS thresholds

- Minimize the steps required to configure DDoS settings
- Automatically adjusts threshold values as patterns change
- Uses machine learning to ensure greater accuracy



Security ›› DoS Protection : Device Configuration

Properties

Log Publisher	None ▾

Auto Threshold

Threshold Bias	Permissive 0 — 100 Paranoid 50
Smoothing	More 0 — 100

Update

Category	Attack Type
Bad Header - DNS	
Bad Header - ICMP	
Bad Header - IGMP	
Bad Header - IPv4	
Bad Header - IPv6	
Bad Header - L2	
Bad Header - TCP	
Bad Header - UDP	
DNS	
Flood	ARP Flood Ethernet Broadcast Packet Ethernet Multicast Packet ICMPv4 flood ICMPv6 flood IGMP Flood IGMP Fragment Flood IPv6 Fragment Flood IP Fragment Flood Routing Header Type 0 TCP BADACK Flood TCP RST Flood TCP SYN ACK Flood TCP SYN Flood TCP Window Size Tsunami SYN UDP Flood
Fragmentation	
Single Endpoint	
SIP	
Bad Header - SCTP	
Other	

Security ›› DoS Protection : Device Configuration ›› TCP RST Flood

Select auto or manual

Properties

Attack Type	TCP RST Flood

● Auto Threshold Configuration ○ Manual Configuration

Attack Detection Floor (PPS)	0
Attack Rate Limit Cieling (PPS)	Infinite ▾
Computed Thresholds	Detection Threshold (PPS) : 10000 Rate Limit (PPS) : Minimum (PPS) : 1000 Current (PPS) : 1000 Maximum (PPS) : 100000 Refresh
Manual Settings	Detection Threshold (PPS) : 12000 Rate Limit (PPS) : 2500

Update

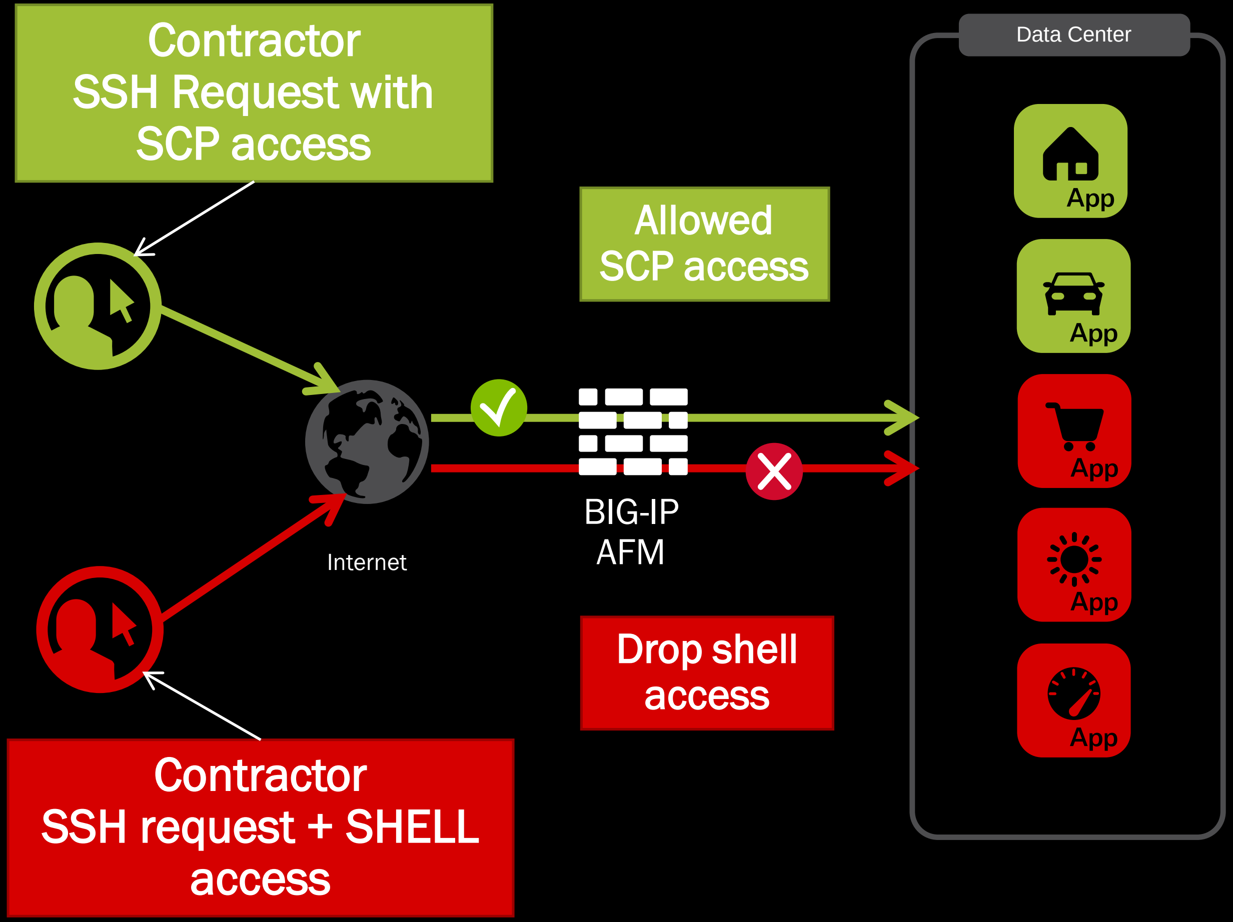
SSH Proxy

Requirement

- Bring visibility into SSH
- Detect and control commands

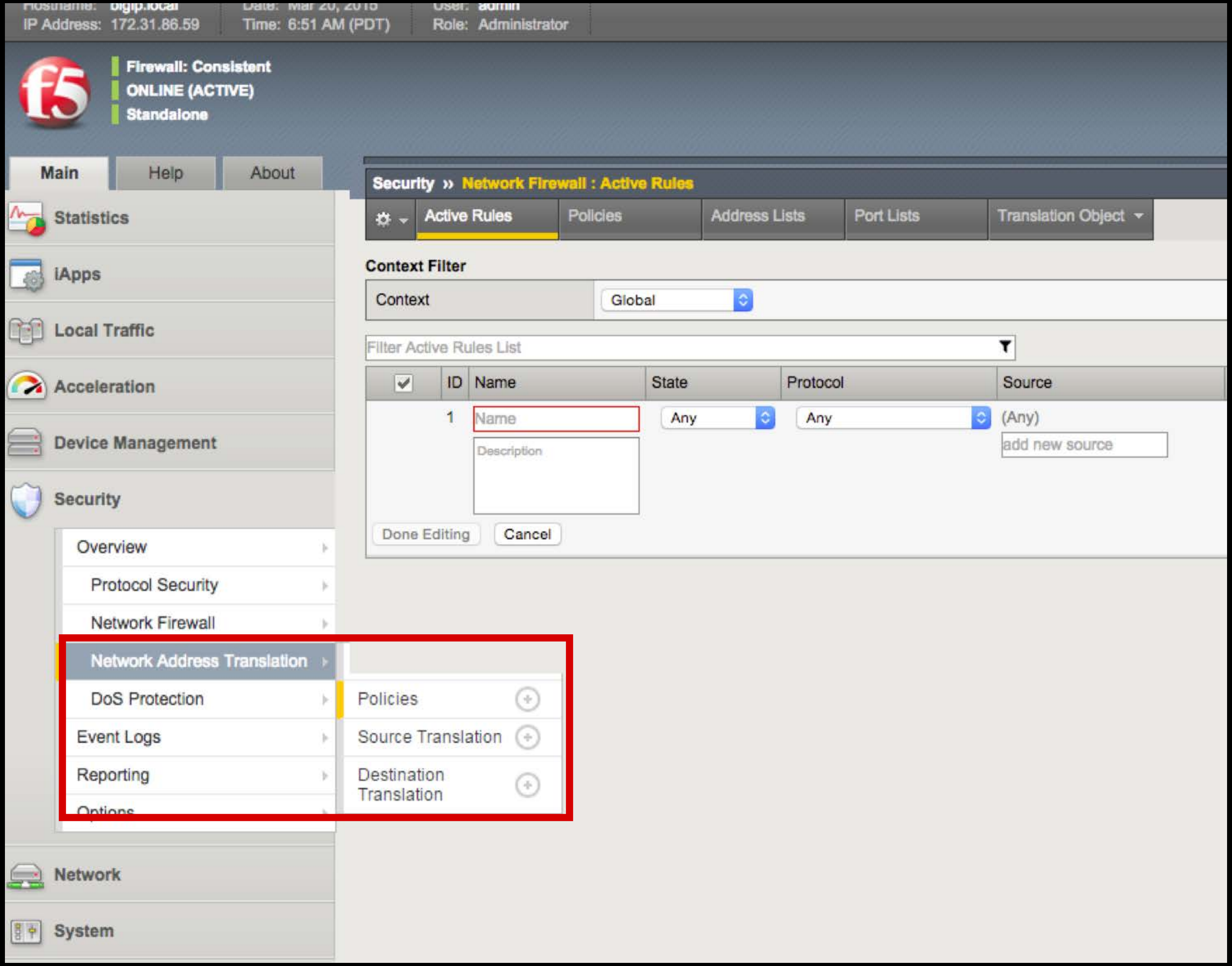
Solution

- Policy based SSH control
- Fine grained, per-user



Streamline NAT Firewall Workflows

- Firewall-centric workflow for NAT
- Easy mapping of IP’s/ports between networks
- Configured with single GUI pane



Hostname: bigip.local Date: Mar 20, 2015 User: admin
IP Address: 172.31.86.59 Time: 6:51 AM (PDT) Role: Administrator

Firewall: Consistent
ONLINE (ACTIVE)
Standalone

Security » Network Firewall : Active Rules

Context Filter

Context: Global

	ID	Name	State	Protocol	Source
☑	1	Name Description	Any	Any	(Any) add new source

BIG-IP AFM Summary

Protect

Industry leading, high performance DoS protection

Visibility

Deep inspection of common protocols used on the internet

Usability

JavaScript based GUI enhancements, with many auto-tuning features

Application Security Manager (ASM)

ASM 12.x Highlights

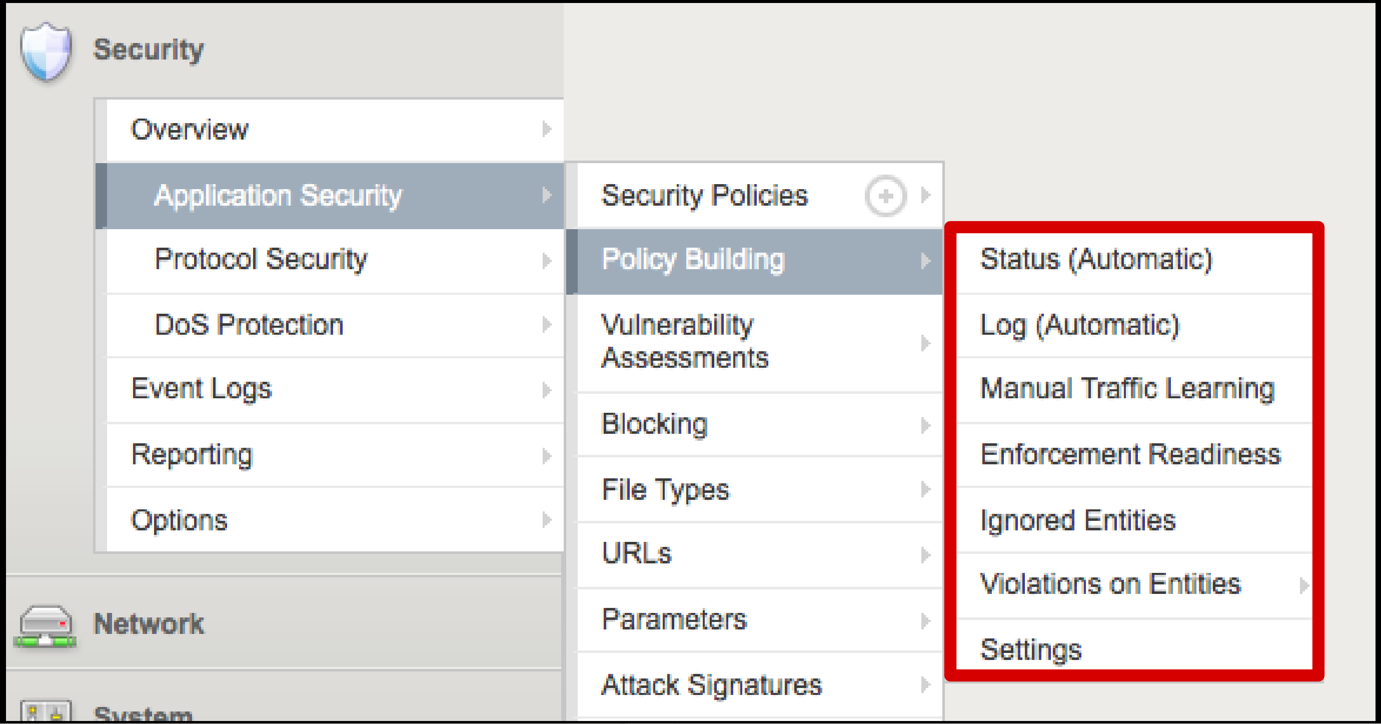
Unified Interface

WebSocket Support

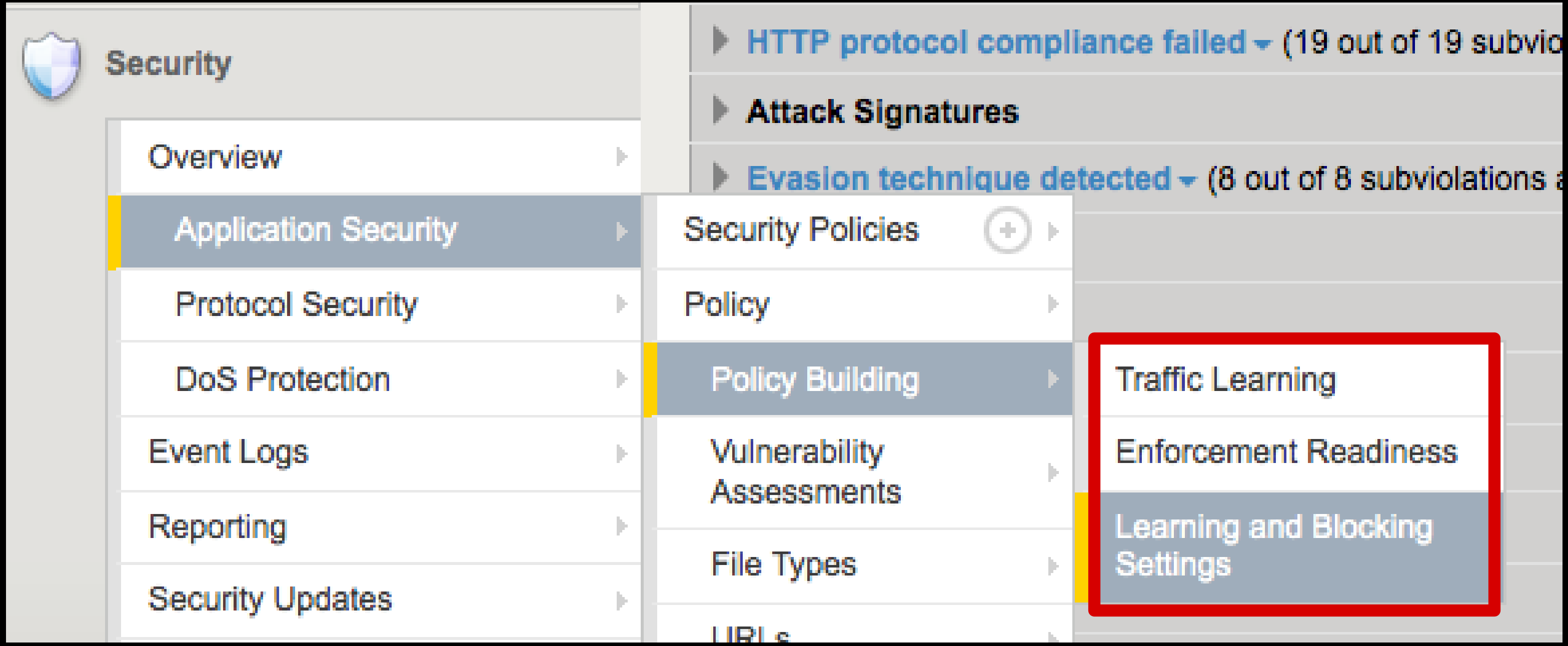
Unified Learning and Policy Building

- New framework for creating a policy, both manually and automatically
- Learning, Blocking, and Policy Settings have been integrated together
- Traffic Learning has been completely overhauled for a simplified workflow

11.6

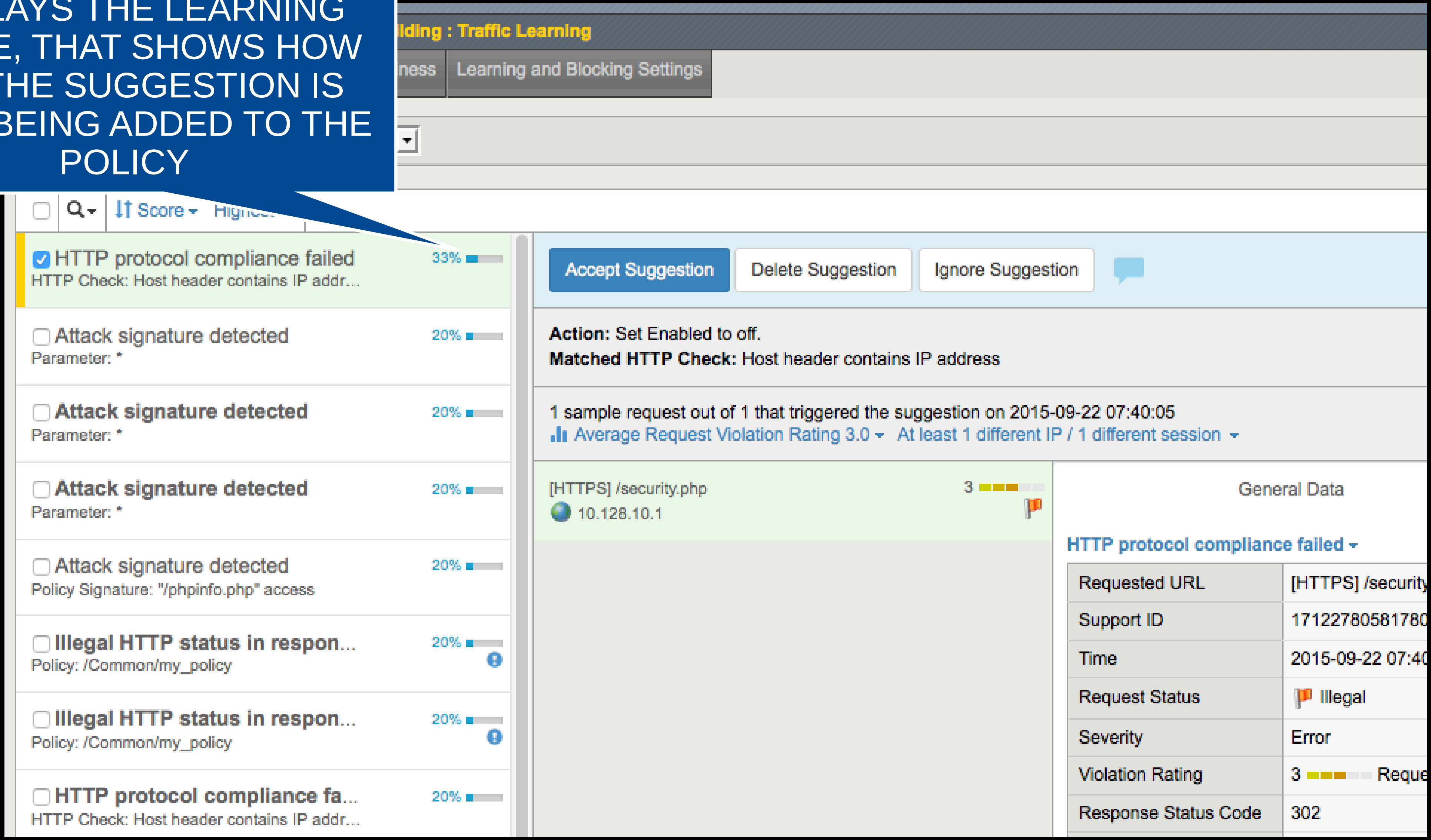

Security
Overview
Application Security
Protocol Security
DoS Protection
Event Logs
Reporting
Options
Network
System
Security Policies
Policy Building
Vulnerability Assessments
Blocking
File Types
URLs
Parameters
Attack Signatures
Status (Automatic)
Log (Automatic)
Manual Traffic Learning
Enforcement Readiness
Ignored Entities
Violations on Entities
Settings

12.0


Security
Overview
Application Security
Protocol Security
DoS Protection
Event Logs
Reporting
Security Updates
HTTP protocol compliance failed (19 out of 19 subvio
Attack Signatures
Evasion technique detected (8 out of 8 subviolations a
Security Policies
Policy
Policy Building
Vulnerability Assessments
File Types
URLs
Traffic Learning
Enforcement Readiness
Learning and Blocking Settings

Traffic Learning

DISPLAYS THE LEARNING SCORE, THAT SHOWS HOW FAR THE SUGGESTION IS FROM BEING ADDED TO THE POLICY



☑ HTTP protocol compliance failed 33%
HTTP Check: Host header contains IP addr...

□ Attack signature detected 20%
Parameter: *

□ **Attack signature detected** 20%
Parameter: *

□ **Attack signature detected** 20%
Parameter: *

□ Attack signature detected 20%
Policy Signature: "/phpinfo.php" access

□ **Illegal HTTP status in respon...** 20%
Policy: /Common/my_policy

□ **Illegal HTTP status in respon...** 20%
Policy: /Common/my_policy

□ **HTTP protocol compliance fa...** 20%
HTTP Check: Host header contains IP addr...

Action: Set Enabled to off.
Matched HTTP Check: Host header contains IP address

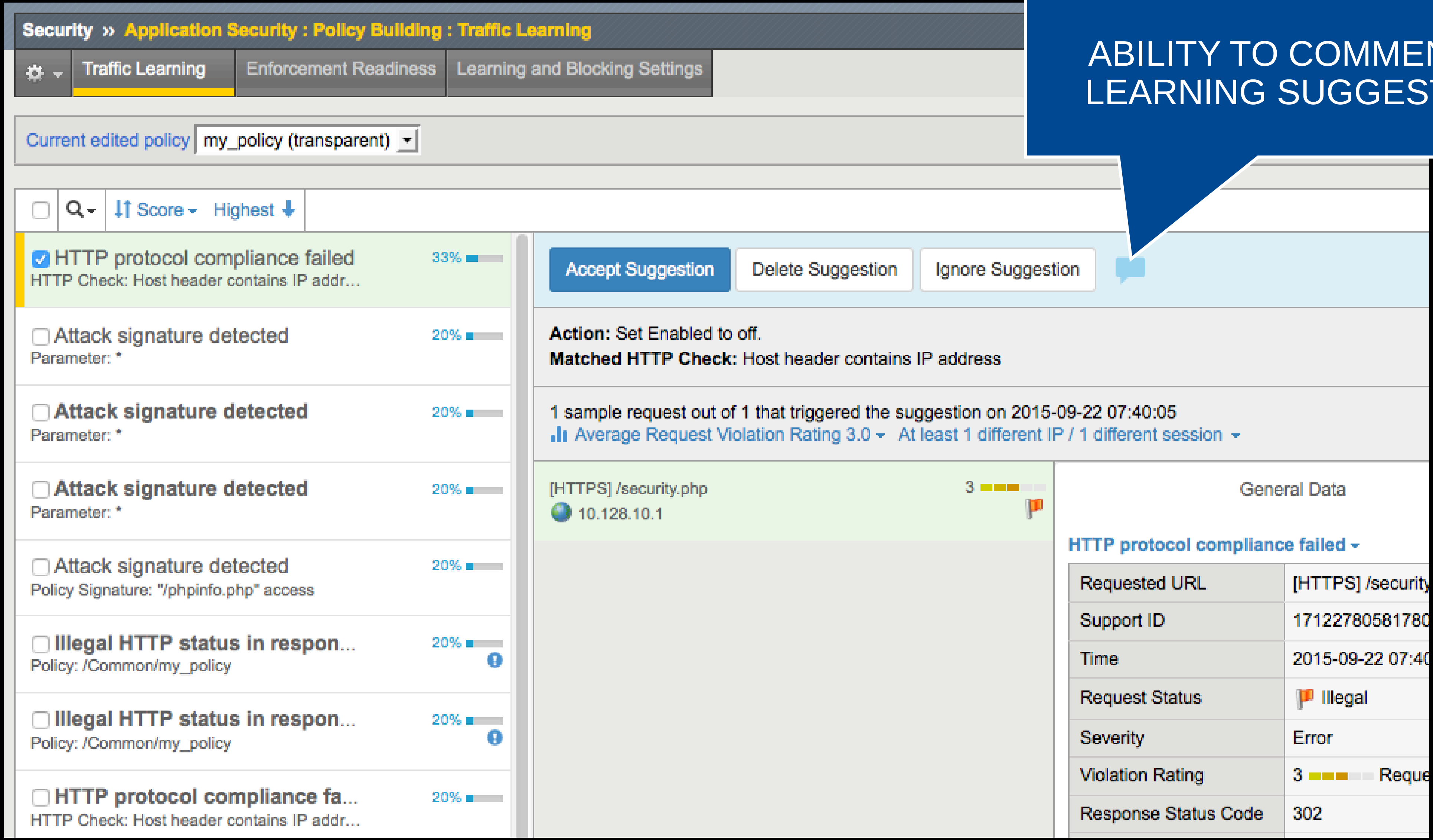
1 sample request out of 1 that triggered the suggestion on 2015-09-22 07:40:05
Average Request Violation Rating 3.0 At least 1 different IP / 1 different session

[HTTPS] /security.php 3
10.128.10.1

HTTP protocol compliance failed

Requested URL	[HTTPS] /security
Support ID	17122780581780
Time	2015-09-22 07:40
Request Status	Illegal
Severity	Error
Violation Rating	3 Reque
Response Status Code	302

Traffic Learning



Security » Application Security : Policy Building : Traffic Learning

Current edited policy: my_policy (transparent)

- ☑ HTTP protocol compliance failed 33%
  HTTP Check: Host header contains IP addr...
- □ Attack signature detected 20%
  Parameter: *
- □ **Attack signature detected** 20%
  Parameter: *
- □ **Attack signature detected** 20%
  Parameter: *
- □ Attack signature detected 20%
  Policy Signature: "/phpinfo.php" access
- □ **Illegal HTTP status in respon...** 20%
  Policy: /Common/my_policy
- □ **Illegal HTTP status in respon...** 20%
  Policy: /Common/my_policy
- □ **HTTP protocol compliance fa...** 20%
  HTTP Check: Host header contains IP addr...

Action: Set Enabled to off.
Matched HTTP Check: Host header contains IP address

1 sample request out of 1 that triggered the suggestion on 2015-09-22 07:40:05
Average Request Violation Rating 3.0 At least 1 different IP / 1 different session

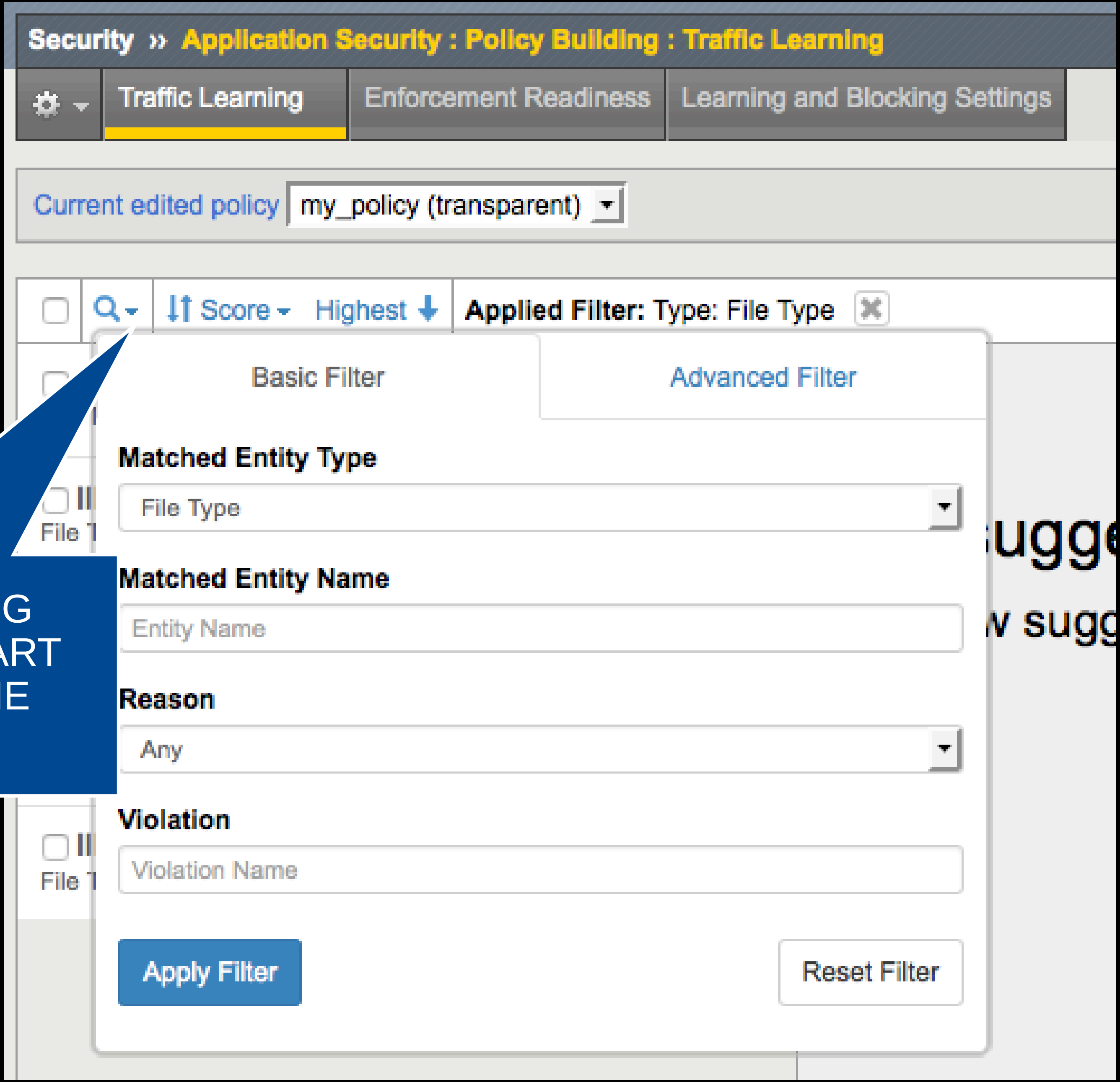
[HTTPS] /security.php 3
10.128.10.1

General Data

HTTP protocol compliance failed

Requested URL	[HTTPS] /security
Support ID	17122780581780
Time	2015-09-22 07:40
Request Status	Illegal
Severity	Error
Violation Rating	3 Reque
Response Status Code	302

ABILITY TO COMMENT ON LEARNING SUGGESTIONS



Security » Application Security : Policy Building : Traffic Learning

Current edited policy: my_policy (transparent)

Applied Filter: Type: File Type

Matched Entity Type: File Type

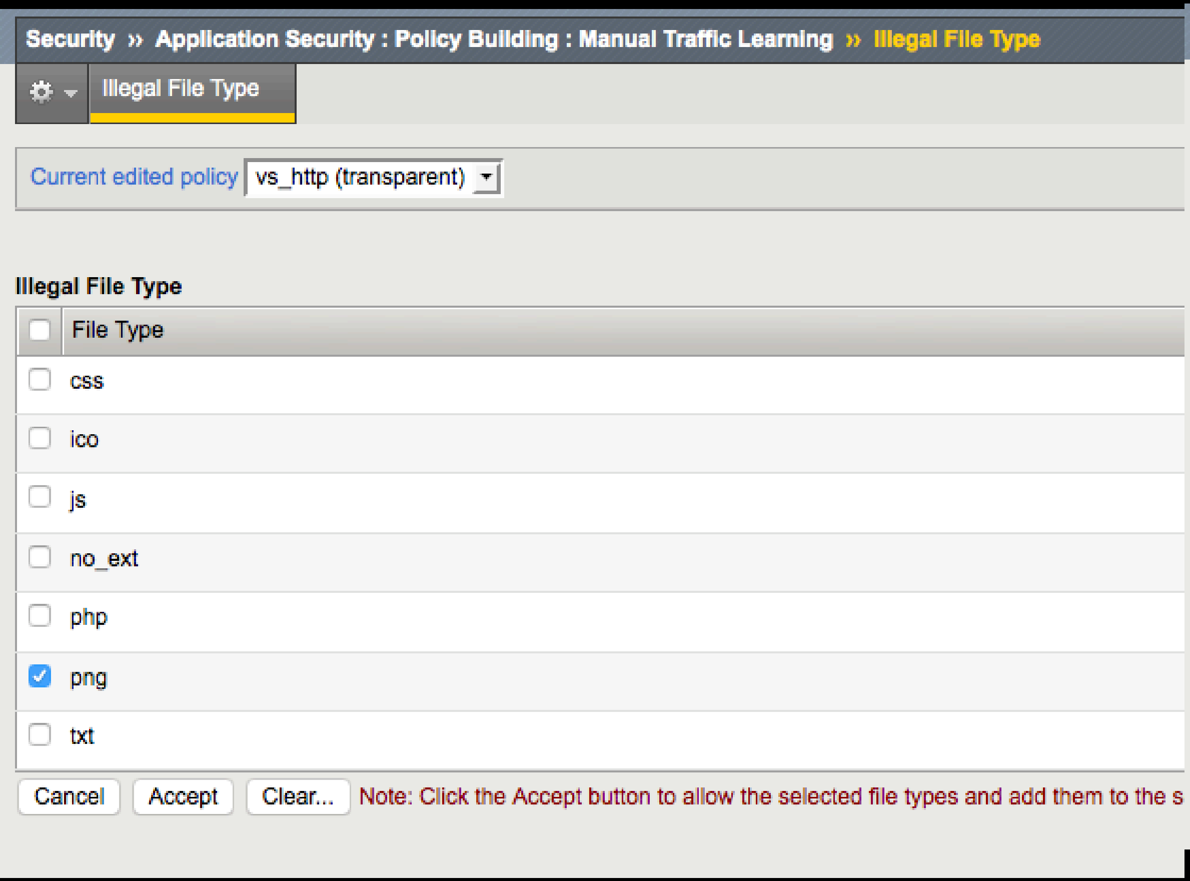
Matched Entity Name: Entity Name

Reason: Any

Violation: Violation Name

FILTER THE LEARNING SUGGESTIONS TO START ADDING THEM TO THE POLICY

11.6



Security » Application Security : Policy Building : Manual Traffic Learning » Illegal File Type

Illegal File Type

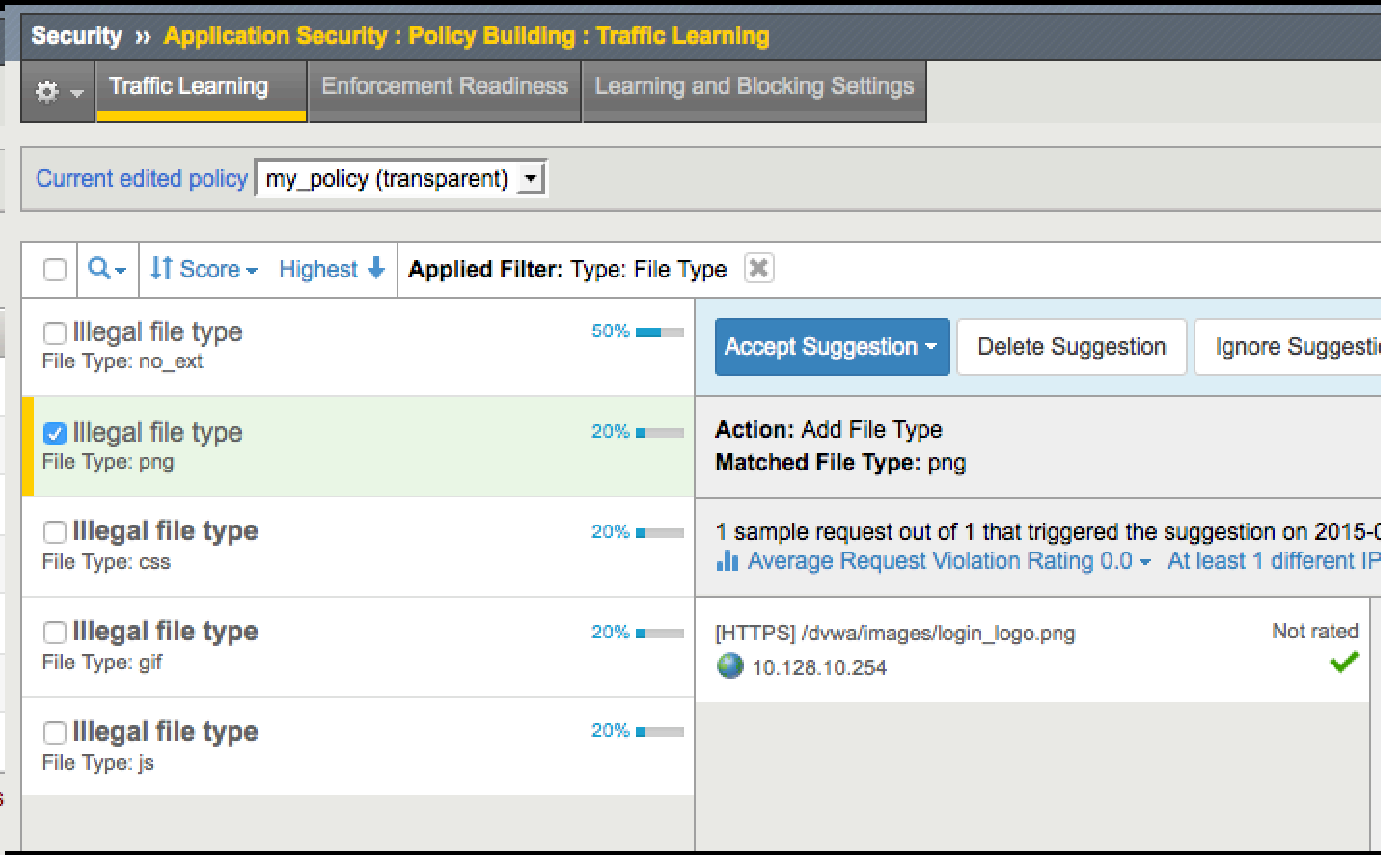
Current edited policy: vs_http (transparent)

Illegal File Type

☐	File Type
☐	css
☐	ico
☐	js
☐	no_ext
☐	php
☑	png
☐	txt

Cancel | Accept | Clear... Note: Click the Accept button to allow the selected file types and add them to the s

12.0



Security » Application Security : Policy Building : Traffic Learning

Traffic Learning | Enforcement Readiness | Learning and Blocking Settings

Current edited policy: my_policy (transparent)

☐ Score Highest **Applied Filter:** Type: File Type

Suggestion	Score
☐ Illegal file type File Type: no_ext	50%
☑ Illegal file type File Type: png	20%
☐ Illegal file type File Type: css	20%
☐ Illegal file type File Type: gif	20%
☐ Illegal file type File Type: js	20%

Accept Suggestion | Delete Suggestion | Ignore Suggesti

Action: Add File Type
Matched File Type: png

1 sample request out of 1 that triggered the suggestion on 2015-0

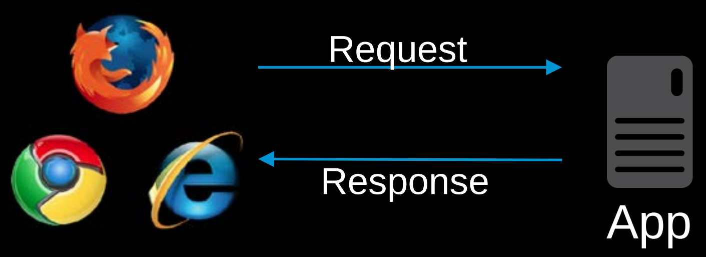
Average Request Violation Rating 0.0 At least 1 different IP

[HTTPS] /dvwa/images/login_logo.png Not rated ✓
10.128.10.254

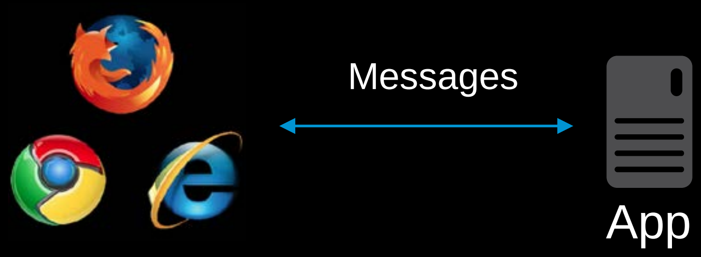
What’s a WebSocket?

- IETF Standard, ratified in 2011
- Light-weight protocol, layered onto **TCP**
- Provides **full duplex** communication between a host and client over TCP
- Allows rich, real-time, reactive user experiences online

HTTP



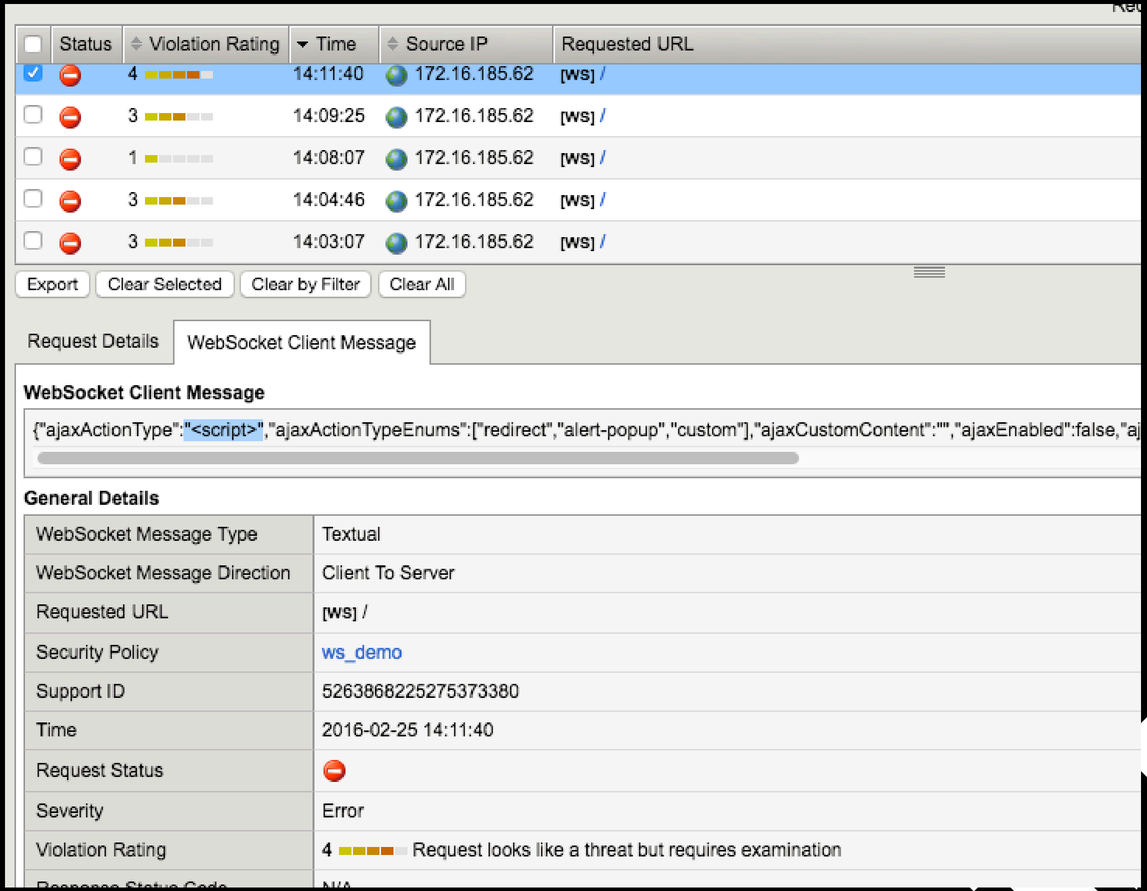
WebSocket



WebSocket Security

The industry’s 1st WAF to protect WebSocket communications

- **Automatically** detect and protect WebSocket traffic
- **Visibility** for WebSocket messages with full message logging
- Supports both **WS** and **WSS**



□	Status	Violation Rating	Time	Source IP	Requested URL
☑	⛔	4	14:11:40	172.16.185.62	[ws] /
□	⛔	3	14:09:25	172.16.185.62	[ws] /
□	⛔	1	14:08:07	172.16.185.62	[ws] /
□	⛔	3	14:04:46	172.16.185.62	[ws] /
□	⛔	3	14:03:07	172.16.185.62	[ws] /

WebSocket Client Message

```
{"ajaxActionType":"<script>","ajaxActionTypeEnums":["redirect","alert-popup","custom"],"ajaxCustomContent":"","ajaxEnabled":false,"aj
```

General Details

WebSocket Message Type	Textual
WebSocket Message Direction	Client To Server
Requested URL	[ws] /
Security Policy	ws_demo
Support ID	5263868225275373380
Time	2016-02-25 14:11:40
Request Status	⛔
Severity	Error
Violation Rating	4 Request looks like a threat but requires examination
Response Status Code	N/A

BIG-IP ASM Summary

Leading-Edge

Keeping up with industry developments as they become widespread

Usability

JavaScript based GUI enhancements, with many auto-tuning features

12.0/12.1 Conclusion

- The 12.1 version of TMOS is a high-stability, long lived release
- Huge improvements to BIG-IP TCO through ease of manageability and superior performance
- Security and Cloud integration enhancements
- Greater programmability with new iApp/iRule LX framework

SOLUTIONS FOR AN APPLICATION WORLD